

SPHEREON 4500

McDATA®
Sphereon™ 4500 Fabric Switch
Installation and Service Manual

P/N 620-000159-320
REV A

Simplifying Storage Network Management

Record of Revisions and Updates

Revision	Date	Description
620-000159-000	8/2002	Initial release of the manual to support early-ship products.
620-000159-100	10/2002	General availability (GA) release of the manual. Describes Release 6.3 of the Enterprise Fabric Connectivity Manager application.
620-000159-200	2/2003	Revision of the manual to describe additional features, Release 7.0, and Release 7.1 of the Enterprise Fabric Connectivity Manager application.
620-000159-201	6/2003	Revision of the manual to describe new firmware and software download procedures from McDATA's home page.
620-000159-300	8/2003	Revision of the manual to describe the one unit (1U) rack-mount server and Release 7.2 of the Enterprise Fabric Connectivity Manager application.
620-000159-310	12/2003	Revision of the manual to describe product management through the SANavigator application and Release 8.1 of the Enterprise Fabric Connectivity Manager application.
620-000159-320	1/2005	Revision of the manual to describe updates for EFCM 8.5 and EOS 7.0.

Copyright © 2002, 2005 McDATA Corporation. All rights reserved.

Printed January 2005

Seventh Edition

No part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without prior written consent of McDATA Corporation.

The information contained in this document is subject to change without notice. McDATA Corporation assumes no responsibility for any errors that may appear.

All computer applications, including but not limited to microcode, described in this document are furnished under a license, and may be used or copied only in accordance with the terms of such license. McDATA either owns or has the right to license the computer applications described in this document. McDATA Corporation retains all rights, title, and interest in the computer applications.

McDATA Corporation makes no warranties, expressed or implied, by operation of law or otherwise, relating to this document, the products or the computer applications described herein. McDATA CORPORATION DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. In no event shall McDATA Corporation be liable for (a) incidental, indirect, special, or consequential damages or (b) any damages whatsoever resulting from the loss of use, data or profits, arising out of this document, even if advised of the possibility of such damages.

Preface	xix
----------------------	-----

Chapter 1 General Information

Switch Description.....	1-2
Field-Replaceable Units	1-3
SFP Transceiver	1-4
Power Supply Assembly	1-5
Controls, Connectors, and Indicators	1-5
IML/Reset Button.....	1-6
Ethernet LAN Connector.....	1-6
Power and System Error LEDs	1-6
FRU Status LEDs.....	1-7
Maintenance Port.....	1-7
Switch Specifications	1-7
Maintenance Approach.....	1-9
Switch Management.....	1-10
SANpilot Interface	1-11
Management Server	1-11
Client PC or Workstation.....	1-12
Error-Detection, Reporting, and Serviceability Features	1-15
Software Diagnostic Features.....	1-17
SANpilot Interface	1-17
Management Server	1-19
SNMP Trap Message Support	1-23
E-Mail and Call-Home Support.....	1-23
Tools and Test Equipment.....	1-24
Tools Supplied with the Switch	1-24
Tools Supplied by Service Personnel	1-25

Chapter 2 **Installation Tasks**

Factory Defaults	2-1
Installation Options	2-2
Summary of Installation Tasks	2-3
Task 1: Verify Installation Requirements	2-4
Task 2: Unpack, Inspect, and Install the Ethernet Hub (Optional). 2-5	
Unpack and Inspect the Ethernet Hub	2-6
Desktop Installation	2-6
Rack-Mount Installation	2-8
Task 3: Unpack, Inspect, and Install the Switch	2-10
Unpack and Inspect the Switch	2-10
Desktop Installation	2-10
Rack-Mount Installation	2-12
Task 4: Configure the Switch at the SANpilot Interface (Optional) 2-13	
Configure Switch Ports	2-15
Configure Switch Identification	2-17
Configure Date and Time	2-18
Configure Operating Parameters	2-19
Configure Fabric Parameters	2-21
Configure Network Information	2-24
Configure SNMP	2-26
Enable or Disable the CLI	2-28
Enable or Disable Host Control	2-29
Configure User Rights	2-30
Configure Port Binding	2-31
Configure Switch Binding	2-32
Configure Fabric Binding	2-34
Enable or Disable Enterprise Fabric Mode	2-35
Configure OpenTrunking	2-36
Install PFE Keys (Optional)	2-38
Task 5: Configure Switch Network Information (Optional)	2-41
Task 6: Unpack, Inspect, and Install the Management Server	2-47
Task 7: Configure Server Password and Network Addresses	2-51
Configure Password	2-51
Configure Private LAN Addresses	2-52
Configure Public LAN Addresses (Optional)	2-54
Task 8: Configure Management Server Information	2-55
Access the Management Server Desktop	2-55
Configure Management Server Names	2-58
Configure Gateway and DNS Server Addresses	2-60
Task 9: Configure Windows 2000 Users	2-63

Change Default Administrator Password	2-64
Add a New User.....	2-65
Change User Properties	2-67
Task 10: Set Management Server Date and Time.....	2-69
Task 11: Configure the Call-Home Feature (Optional)	2-71
Task 12: Assign User Names and Passwords.....	2-72
Task 13: Configure the Switch to the Management Application.....	2-76
Task 14: Record or Verify Server Restore Information.....	2-78
Task 15: Verify Switch-to-Server Communication.....	2-80
Task 16: Configure PFE Key (Optional)	2-82
Task 17: Configure Management Server (Optional).....	2-86
Task 18: Set Switch Date and Time	2-86
Task 19: Configure the Sphereon 4500 Element Manager Application.....	2-88
Configure Switch Identification.....	2-89
Configure Switch Parameters.....	2-90
Configure Fabric Parameters.....	2-92
Configure Preferred Paths	2-94
Configure Switch Binding	2-96
Configure Switch Ports	2-101
Configure SNMP Trap Message Recipients	2-103
Configure Threshold Alerts.....	2-105
Configure OpenTrunking	2-109
Enable SANpilot Interface and Telnet Access.....	2-112
Configure, Enable, and Test E-mail Notification	2-112
Configure and Enable Ethernet Events.....	2-114
Configure, Enable, and Test Call-Home Event Notification.....	2-114
Task 20: Back Up Configuration Data	2-115
Task 21: Cable Fibre Channel Ports	2-120
Task 22: Configure Zoning (Optional)	2-121
Configure Zones (SANpilot Interface).....	2-121
Configure Zone Sets (SANpilot Interface).....	2-124
Task 23: Connect Switch to a Fabric Element (Optional).....	2-125
Task 24: Register with the McDATA File Center	2-127

Chapter 3

Diagnostics

Maintenance Analysis Procedures.....	3-1
Factory Defaults	3-1
Quick Start	3-2
MAP 0000: Start MAP	3-6

MAP 0100: Power Distribution Analysis	3-30
MAP 0200: POST Failure Analysis	3-38
MAP 0300: Server Application Problem Determination.....	3-41
MAP 0400: Loss of Server Communication	3-51
MAP 0500: FRU Failure Analysis	3-68
MAP 0600: Port Failure and Link Incident Analysis	3-74
MAP 0700: Fabric, ISL, and Segmented Port Problem Determination	3-93
MAP 0800: Server Hardware Problem Determination.....	3-110

Chapter 4 **Repair Information**

Procedural Notes	4-2
Repair Procedures.....	4-2
Obtain Log Information.....	4-2
SANpilot Logs.....	4-3
Viewing the Security Log	4-7
Viewing the Audit Log	4-8
Viewing the Fabric Log.....	4-9
Viewing the Embedded Port Frame Log.....	4-10
Viewing All Logs	4-12
SAN Management Logs.....	4-13
Element Manager Logs.....	4-16
Obtain Port Diagnostic Information	4-21
Port LEDs.....	4-21
SANpilot Interface.....	4-22
Management Server	4-30
Perform Port Diagnostic Loopback Tests	4-38
Internal Loopback Test (SANpilot Interface).....	4-38
External Loopback Test (SANpilot Interface).....	4-40
Internal Loopback Test (Management Server)	4-41
External Loopback Test (Management Server)	4-43
Collect Maintenance Data.....	4-44
SANpilot Interface.....	4-45
Management Server	4-47
Set the Switch Online or Offline	4-48
Set Online State (SANpilot Interface)	4-49
Set Offline State (SANpilot Interface).....	4-49
Set Online State (Management Server).....	4-50
Set Offline State (Management Server)	4-50
Block or Unblock a Port	4-51
Block a Port (SANpilot Interface).....	4-51
Unblock a Port (SANpilot Interface).....	4-52

Block a Port (Management Server).....	4-52
Unblock a Port (Management Server).....	4-53
Clean Fiber-Optic Components.....	4-54
Power-On Procedure	4-55
Power-Off Procedure	4-56
IML, IPL, or Reset the Switch	4-56
Switch IML.....	4-57
Switch IPL	4-58
Switch Reset.....	4-58
Manage Firmware Versions	4-59
SANpilot Interface	4-59
Management Server.....	4-68
Manage Configuration Data	4-79
Back Up the Configuration	4-79
Restore the Configuration.....	4-80
Reset Configuration Data (SANpilot Interface).....	4-82
Reset Configuration Data (Management Server)	4-84
Install or Upgrade Software.....	4-87

Chapter 5 FRU Removal and Replacement

Procedural Notes	5-1
Remove and Replace FRUs.....	5-2
RRP 1: SFP Optical Transceiver.....	5-2
RRP 2: Redundant Power Supply.....	5-6

Chapter 6 Illustrated Parts Breakdown

Front-Accessible FRUs.....	6-2
Rear-Accessible FRUs	6-3
Miscellaneous Parts	6-4
Power Cords and Receptacles	6-5

Appendix A Messages

Sphereon 4500 Element Manager Messages	A-1
A	A-1
C.....	A-3
D	A-11
E.....	A-12
F	A-14
I.....	A-15
L.....	A-20
M.....	A-20

N.....	A-21
P.....	A-22
R.....	A-23
S.....	A-24
T.....	A-25
U.....	A-29
Y.....	A-29

Appendix B Event Code Tables

System Events (000 through 199)	B-2
Power Supply Events (200 through 299)	B-20
Fan Events (300 through 399)	B-23
CTP Card Events (400 through 499)	B-29
Port Events (500 through 599)	B-35
Thermal Sensor Events (800 through 899)	B-43

Appendix C Restore Management Server

Requirements	C-1
Restore Management Server Procedure	C-2

Appendix D Consolidating Management Servers

Overview.....	D-1
Required SAN Management Application Version.....	D-3
IP Address Assignment	D-3
Consolidating Management Servers.....	D-5
Common Steps for All Configurations.....	D-5
Private LAN Connection	D-13
Private and Public LAN Connection	D-15
Reconfiguring a Client PC After a Management Server Failure.....	D-19

Index.....	1
-------------------	----------

1-1	Sphereon 4500 Switch	1-2
1-2	Sphereon 4500 Switch (Front View)	1-3
1-3	Sphereon 4500 Switch (Rear View)	1-4
1-4	Management Server	1-11
1-5	24-Port Ethernet Hub	1-12
1-6	Typical Network Configuration (One Ethernet Connection)	1-13
1-7	Typical Network Configuration (Two Ethernet Connections)	1-14
1-8	View Panel (SANpilot Interface)	1-18
1-9	Main Window (SANavigator or EFCM)	1-19
1-10	Sphereon 4500 Product Icon	1-21
1-11	Hardware View	1-22
1-12	Loopback Plug	1-24
1-13	Fiber-Optic Protective Plug	1-25
1-14	Null Modem Cable	1-25
2-1	Stacked Ethernet Hubs	2-7
2-2	Patch Cable and MDI Selector Configuration	2-7
2-3	Mounting Bracket Installation (Ethernet Hub)	2-8
2-4	Rack Installation (Ethernet Hub)	2-9
2-5	AC Power Connections	2-11
2-6	Enter Network Password Dialog Box	2-14
2-7	View Panel (Director Page)	2-15
2-8	Configure Panel (Ports Page)	2-16
2-9	Configure Panel (Switch Page with Identification Tab)	2-18
2-10	Configure Panel (Switch Page with Date/Time Tab)	2-19
2-11	Configure Panel (Switch Page with Parameters Tab)	2-20
2-12	Configure Panel (Switch Page with Fabric Parameters Tab)	2-22
2-13	Configure Panel (Switch Page with Network Tab)	2-25
2-14	Network Information Message Box	2-25

2-15	Configure Panel (Management Page with SNMP Tab)	2-27
2-16	Configure Panel (Management Page with CLI Tab)	2-28
2-17	Configure Panel (Management Page with OSMS Tab)	2-29
2-18	Configure Panel (Security Page with User Rights Tab)	2-30
2-19	Configure Panel (Security Page with Port Binding Tab)	2-31
2-20	Configure Panel (Security Page with Switch Binding Tab)	2-32
2-21	Configure Panel (Security Page with Fabric Binding Tab)	2-34
2-22	Configure Panel (Security Page with EFM Tab)	2-36
2-23	Configure Panel (Performance Page with OpenTrunking Tab)	2-37
2-24	Operations Panel (Feature Installation Tab)	2-40
2-25	Connection Description Dialog Box	2-43
2-26	Connect To Dialog Box	2-43
2-27	COMn Properties Dialog Box	2-44
2-28	Sphereon 4500 - HyperTerminal Window	2-45
2-29	HyperTerminal Dialog Box (1)	2-46
2-30	HyperTerminal Dialog Box (2)	2-46
2-31	1U Management Server Connections	2-49
2-32	LCD Panel During Boot Sequence	2-50
2-33	LCD Panel (Password Entry)	2-51
2-34	LCD Panel (New Password)	2-52
2-35	LCD Panel (Save Change)	2-52
2-36	LCD Panel (Password Entry)	2-52
2-37	LCD Panel (LAN 2 IP Address)	2-53
2-38	LCD Panel (Save Change)	2-53
2-39	LCD Panel (LAN 2 Subnet Mask)	2-53
2-40	LCD Panel (Save Change)	2-53
2-41	LCD Panel (Password Entry)	2-54
2-42	LCD Panel (LAN 1 IP Address)	2-54
2-43	LCD Panel (Save Change)	2-54
2-44	LCD Panel (LAN 1 Subnet Mask)	2-55
2-45	LCD Panel (Save Change)	2-55
2-46	VNC Authentication Screen	2-56
2-47	Welcome to Windows Dialog Box	2-56
2-48	Log On to Windows Dialog Box	2-57
2-49	SANavigator Log In or EFCM Log In Dialog Box	2-57
2-50	Control Panel Window	2-58
2-51	System Properties Dialog Box (Network Identification Tab)	2-59
2-52	Identification Changes Dialog Box	2-59
2-53	Network and Dial-up Connections Window	2-60
2-54	Local Area Connection 2 Status Dialog Box	2-61
2-55	Local Area Connection 2 Properties Dialog Box	2-61
2-56	Internet Protocol (TCP/IP) Properties Dialog Box	2-62
2-57	Users and Passwords Dialog Box	2-63

2-58	Windows Security Dialog Box	2-64
2-59	Change Password Dialog Box	2-65
2-60	Add New User Wizard (First Window)	2-66
2-61	Add New User Wizard (Second Window)	2-66
2-62	Add New User Wizard (Third Window)	2-67
2-63	MGMTSERVER\sr vacc Properties Dialog Box (General Tab)	2-68
2-64	MGMTSERVER\sr vacc Properties Dialog Box (Group Membership Tab) 2-68	
2-65	Date/Time Properties Dialog Box (Date & Time Tab)	2-69
2-66	Date/Time Properties Dialog Box (Time Zone Tab)	2-70
2-67	Call Home Configuration Dialog Box	2-71
2-68	Main Window (SANavigator or EFCM)	2-73
2-69	SANavigator or EFCM 8 Server Users Dialog Box	2-74
2-70	Add User Dialog Box	2-74
2-71	Discover Setup Dialog Box	2-76
2-72	Domain Information Dialog Box (IP Address Page)	2-77
2-73	System Properties Dialog Box (General Tab)	2-79
2-74	Sphereon 4500 Product Icon	2-80
2-75	Hardware View	2-81
2-76	No Feature Key Dialog Box	2-83
2-77	Hardware View (with Element Manager Message)	2-83
2-78	Configure Feature Key Dialog Box	2-84
2-79	New Feature Key Dialog Box	2-84
2-80	Enable Feature Key Dialog Box	2-85
2-81	Warning Dialog Box	2-85
2-82	Configure Date and Time Dialog Box	2-87
2-83	Date and Time Synced Dialog Box	2-88
2-84	Configure Identification Dialog Box	2-89
2-85	Configure Switch Parameters Dialog Box	2-91
2-86	Configure Fabric Parameters Dialog Box	2-92
2-87	Configure Preferred Paths Dialog Box	2-95
2-88	Add Preferred Path Dialog Box	2-95
2-89	Switch Binding - State Change Dialog Box	2-98
2-90	Switch Binding - Membership List Dialog Box	2-99
2-91	Display Options Dialog Box	2-100
2-92	Add Detached Node Dialog Box	2-101
2-93	Configure Ports Dialog Box	2-101
2-94	Configure SNMP Dialog Box	2-104
2-95	Configure Threshold Alert(s) Dialog Box	2-105
2-96	New Threshold Alert Dialog Box (Screen 1)	2-106
2-97	New Threshold Alert Dialog Box (Screen 2)	2-107
2-98	New Threshold Alert Dialog Box (Screen 3)	2-108
2-99	New Threshold Alert Dialog Box (Screen 4)	2-109

2-100	Configure OpenTrunking Dialog Box	2-110
2-101	Email Event Notification Setup Dialog Box	2-112
2-102	Configure Ethernet Events Dialog Box	2-114
2-103	Call Home Event Notification Setup Dialog Box	2-115
2-104	InCD Icon (Unformatted CD)	2-117
2-105	InCD Wizard (First Window)	2-117
2-106	InCD Icon (Formatted CD)	2-117
2-107	SANavigator or EFCM Message Dialog Box	2-118
2-108	Shut Down Windows Dialog Box	2-118
2-109	TightVNC Network Error Message	2-119
2-110	Configure Panel (Zoning Page with Zones Tab)	2-122
2-111	Configure Panel (Zoning Page with Modify Zone Tab)	2-123
2-112	Configure Panel (Zoning Page with Zone Set Tab)	2-124
2-113	Port Properties Dialog Box	2-127
2-114	McDATA File Center Home Page	2-128
2-115	McDATA File Center (New User Registration Page)	2-129
3-1	Username and Password Required Dialog Box	3-7
3-2	View Panel (SANpilot Interface)	3-8
3-3	View Panel (Port Properties Tab)	3-10
3-4	View Panel (FRU Properties Tab)	3-12
3-5	Monitor Panel (Log Tab)	3-13
3-6	Shut Down Windows Dialog Box	3-15
3-7	LCD Panel During Boot Sequence	3-16
3-8	SANavigator Login or EFCM Login Dialog Box	3-17
3-9	Main Window (SANavigator or EFCM)	3-17
3-10	Hardware View	3-20
3-11	Port Properties Dialog Box	3-23
3-12	Link Incident Log	3-24
3-13	Event Log	3-25
3-14	Windows Security Dialog Box	3-42
3-15	Windows Task Manager Dialog Box (Applications Page)	3-42
3-16	Shut Down Windows Dialog Box	3-43
3-17	LCD Panel During Boot Sequence	3-44
3-18	SANavigator Login or EFCM Login Dialog Box	3-45
3-19	Dr. Watson for Windows 2000 Dialog Box	3-48
3-20	LCD Panel During Boot Sequence	3-49
3-21	SANavigator Login or EFCM Login Dialog Box	3-50
3-22	Daisy-Chained Ethernet Hubs	3-56
3-23	LCD Panel (LAN 2 IP Address)	3-60
3-24	Connection Description Dialog Box	3-61
3-25	Connect To Dialog Box	3-62
3-26	COMn Properties Dialog Box	3-62

3-27	Sphereon 4500 - HyperTerminal Dialog Box	3-63
3-28	HyperTerminal Dialog Box	3-64
3-29	HyperTerminal Dialog Box	3-64
3-30	Discover Setup Dialog Box	3-65
3-31	Editing Domain Information Dialog Box	3-65
3-32	Domain Information Dialog Box (IP Address Page)	3-66
3-33	SANavigator or EFCM Message Dialog Box	3-67
3-34	Domain Information Dialog Box (IP Address Page)	3-67
3-35	Configure Fabric Parameters Dialog Box	3-85
3-36	Switch Binding - State Change Dialog Box	3-87
3-37	Fabric Binding Dialog Box	3-88
3-38	Switch Binding - Membership List Dialog Box	3-89
3-39	Clear Link Incident Alert(s) Dialog Box	3-91
3-40	Configure Fabric Parameters Dialog Box	3-100
3-41	Configure Switch Parameters Dialog Box	3-101
3-42	Zoning Dialog Box (Zone Library Tab)	3-103
3-43	Zoning Dialog Box (Active Zone Set Tab)	3-104
3-44	SANavigator or EFCM Message Dialog Box	3-111
3-45	Windows Task Manager Dialog Box (Performance Page)	3-112
3-46	Shut Down Windows Dialog Box	3-113
3-47	LCD Panel During Boot Sequence	3-113
3-48	SANavigator Login or EFCM Login Dialog Box	3-115
3-49	LCD Panel During Boot Sequence	3-116
4-1	Monitor Panel (Logs Page)	4-4
4-2	Event Log	4-5
4-3	Open Trunking Re-Route Log	4-6
4-4	Link Incident Log	4-7
4-5	Security Log	4-8
4-6	Viewing the Audit Log	4-9
4-7	Viewing the Fabric Log	4-10
4-8	Viewing the Frame Log	4-11
4-9	Setting Embedded Port Frame Filtering	4-12
4-10	All Logs View	4-13
4-11	Event Log	4-14
4-12	Product Status Log	4-15
4-13	Sphereon 4500 Event Log	4-16
4-14	Hardware Log	4-17
4-15	Link Incident Log	4-18
4-16	Threshold Alert Log	4-19
4-17	Open Trunking Log	4-20
4-18	Monitor Panel (Port List Page)	4-23
4-19	Monitor Panel (Port Stats Page)	4-24

4-20	View Panel (Port Properties Page)	4-29
4-21	Port List View	4-31
4-22	Performance View	4-32
4-23	Port Properties Dialog Box	4-36
4-24	Port Technology Dialog Box	4-37
4-25	Operations Panel (Port Page with Diagnostics Tab)	4-39
4-26	Port Diagnostics Dialog Box	4-42
4-27	Operations Panel (Maintenance Page with System Files Tab)	4-45
4-28	Save As Dialog Box	4-46
4-29	Download Complete Dialog Box	4-46
4-30	Save Data Collection Dialog Box	4-47
4-31	Data Collection Dialog Box	4-48
4-32	Operations Panel (Switch Page with Online State Tab)	4-49
4-33	Set Online State Dialog Box	4-50
4-34	Configure Panel (Ports Page)	4-51
4-35	Warning Dialog Box	4-53
4-36	Warning Dialog Box	4-54
4-37	Clean Fiber-Optic Components	4-54
4-38	Information Dialog Box	4-58
4-39	View Panel (Unit Properties Page)	4-60
4-40	McDATA File Center Home Page	4-61
4-41	McDATA File Center (Login Page)	4-61
4-42	McDATA File Center (Find Documents Page)	4-62
4-43	McDATA File Center (Documents Match Page)	4-63
4-44	McDATA File Center (Current Request Page)	4-63
4-45	McDATA File Center (Request History Page)	4-64
4-46	File Download Dialog Box	4-64
4-47	Save As Dialog Box	4-65
4-48	Download Complete Dialog Box	4-65
4-49	Operations Panel (Maintenance Page with Firmware Upgrade Tab) .	4-66
4-50	Browser-Specific Message Box	4-67
4-51	Firmware Received Message Box	4-67
4-52	Firmware Upgrade Complete Message Box	4-68
4-53	Firmware Library Dialog Box	4-69
4-54	McDATA File Center Home Page	4-70
4-55	McDATA File Center (Find Documents Page)	4-70
4-56	McDATA File Center (Documents Match Page)	4-71
4-57	McDATA File Center (Current Request Page)	4-71
4-58	McDATA File Center (Request History Page)	4-72
4-59	File Download Dialog Box	4-72
4-60	Save As Dialog Box	4-73
4-61	Download Complete Dialog Box	4-73
4-62	Firmware Library Dialog Box	4-74

4-63	New Firmware Version Dialog Box	4-75
4-64	New Firmware Description Dialog Box	4-75
4-65	File Transfer Message Box	4-75
4-66	Firmware Library Dialog Box	4-77
4-67	Warning Dialog Box	4-77
4-68	Send Firmware Dialog Box	4-78
4-69	Backup and Restore Configuration Dialog Box	4-80
4-70	Information Dialog Box	4-80
4-71	Backup and Restore Configuration Dialog Box	4-81
4-72	Warning Dialog Box	4-81
4-73	Information Dialog Box	4-81
4-74	Operations Panel (Switch Page with Reset Config Tab)	4-82
4-75	Browser-Specific Message Box	4-83
4-76	Reset Configuration Dialog Box	4-84
4-77	Discover Setup Dialog Box	4-85
4-78	Domain Information Dialog Box	4-86
4-79	McDATA File Center Home Page	4-88
4-80	McDATA File Center (Find Documents Page)	4-88
4-81	McDATA File Center (Documents Match Page)	4-89
4-82	McDATA File Center (Current Request Page)	4-89
4-83	McDATA File Center (Request History Page)	4-90
4-84	File Download Dialog Box	4-90
4-85	Save As Dialog Box	4-91
4-86	Download Complete Dialog Box	4-91
4-87	Run Dialog Box	4-92
4-88	McDATA EFC Management Applications Dialog Box	4-93
4-89	SANavigator Log In or EFCM Log In Dialog Box	4-94
5-1	SFP Optical Transceiver Removal and Replacement	5-4
5-2	Redundant Power Supply Removal and Replacement	5-7
6-1	Front-Accessible FRUs	6-2
6-2	Rear-Accessible FRUs	6-3
6-3	Miscellaneous Parts	6-4
6-4	Power Cords and Receptacles	6-5
C-1	Run Dialog Box	C-4
C-2	VNC Authentication Screen	C-5
C-3	Welcome to Windows Dialog Box	C-5
C-4	Log On to Windows Dialog Box	C-6
C-5	SANavigator Log In or EFCM Log In Dialog Box	C-7

D-1	Servers Before Consolidation (Private LAN Connection Only)	D-2
D-2	Servers Before Consolidation (Private and Public LAN Connections)	D-2
D-3	IP Addresses in a Multiswitch Environment (Before Consolidation) ..	D-3
D-4	LCD Panel (Password Entry)	D-5
D-5	LCD Panel (LAN 2 IP Address)	D-6
D-6	LCD Panel (Save Change)	D-6
D-7	LCD Panel (LAN 2 Subnet Mask)	D-6
D-8	LCD Panel (Save Change)	D-6
D-9	System Properties Dialog Box (Network Identification Tab)	D-7
D-10	Identification Changes Dialog Box	D-8
D-11	IP Addresses in a Multiswitch Environment (After Consolidation)	D-9
D-12	Discover Setup Dialog Box	D-10
D-13	Domain Information Dialog Box (IP Address Page)	D-11
D-14	Sphereon 4500 Product Icon	D-11
D-15	SANavigator or EFCM Message Dialog Box	D-12
D-16	Patch Cable and MDI Selector Configuration	D-12
D-17	Network and Dial-up Connections Window	D-14
D-18	Local Area Connection Status Dialog Box	D-14
D-19	Servers After Consolidation (Private LAN Connection Only)	D-15
D-20	Shut Down Windows Dialog Box	D-15
D-21	TightVNC Network Error Message	D-16
D-22	VNC Authentication Screen	D-16
D-23	Welcome to Windows Dialog Box	D-17
D-24	Log On to Windows Dialog Box	D-17
D-25	SANavigator Log In or EFCM Log In Dialog Box	D-18
D-26	Servers After Consolidation (Private and Public LAN Connections)	D-19
D-27	My Computer Window	D-20
D-28	Local Disk (C:) Window	D-20

2-1	Factory-Set Defaults (Sphereon 4500 Switch)	2-1
2-2	Factory-Set Defaults (Management Server)	2-2
2-3	Installation Task Summary	2-3
2-4	Switch Operational States and Symbols	2-80
3-1	Factory-Set Defaults	3-2
3-2	MAP Summary	3-2
3-3	Event Codes versus Maintenance Action	3-3
3-4	MAP 100 Event Codes	3-30
3-5	MAP 200 Event Codes	3-39
3-6	MAP 200 Byte 0 FRU Codes	3-39
3-7	MAP 400 Error Messages	3-55
3-8	MAP 500 Event Codes	3-69
3-9	MAP 600 Event Codes	3-75
3-10	Port Operational States and Actions (SANpilot)	3-78
3-11	Port Operational and LED States (Management Server)	3-80
3-12	Invalid Attachment Reasons and Actions	3-82
3-13	MAP 700 Event Codes	3-94
3-14	Port Segmentation Reasons and Actions (SANpilot)	3-95
3-15	Port Segmentation Reasons and Actions (Management Server)	3-97
3-16	Byte 4 Segmentation Reasons and Actions	3-99
3-17	Bytes 8 through 11 Failure Reasons and Actions	3-108
4-1	Port Operational States	4-21
5-1	Concurrent FRUs	5-2
6-1	Front-Accessible FRU Parts List	6-2

6-2 Rear-Accessible FRU Parts List 6-3

6-3 Miscellaneous Parts List 6-4

6-4 Power Cord and Receptacle List 6-6

This publication is part of a documentation suite that supports the McDATA® Sphereon 4500 Fabric Switch.

Who Should Use this Manual



Use this publication if you are a trained installation and service representative experienced with the switch, storage area network (SAN) technology, and Fibre Channel technology.

The Sphereon 4500 Fabric Switch contains no customer-serviceable parts that require internal access to the product during normal operation or prescribed maintenance conditions. In addition, refer to this manual for instructions prior to performing any maintenance action.

Organization of this Manual

This publication includes six chapters and four appendices organized as follows:

Chapter 1, *General Information* - This chapter describes the switch, including field-replaceable units (FRUs), controls, connectors, and indicators, and switch specifications. The chapter also describes the maintenance approach, switch management through the SANpilot interface, rack-mount management server, or a remote workstation, error detection and reporting features, serviceability features, software diagnostic features, and tools and test equipment.

Chapter 2, *Installation Tasks* - This chapter describes tasks to install, configure, and verify operation of the switch, optional Ethernet hub, and rack-mount management server.

[Chapter 3, *Diagnostics*](#) - This chapter describes maintenance analysis procedures (MAPs) to fault isolate a switch problem to an individual FRU.

[Chapter 4, *Repair Information*](#) - This chapter describes supplementary diagnostic and repair procedures for a failed switch. The chapter includes procedures to display and use log information, perform port diagnostics, manage configuration data, collect maintenance data, power-on, power-off, and reset the switch, set the switch online or offline, block ports, manage switch firmware, clean fiber optics, and install or upgrade management server software.

[Chapter 5, *FRU Removal and Replacement*](#) - This chapter describes procedures to remove and replace switch FRUs.

[Chapter 6, *Illustrated Parts Breakdown*](#) - This chapter illustrates, describes, and shows the location of switch FRUs. In addition, switch FRUs are cross-referenced to corresponding part numbers.

[Appendix A, *Messages*](#) - This appendix provides a list of user and error messages that appear at the Sphereon 4500 Element Manager application at the management server. A description of each message and a recommended course of action in response to the message are also provided.

[Appendix B, *Event Code Tables*](#) - This appendix provides an explanation of event codes that appear at the SANpilot interface or Sphereon 4500 Element Manager application. The event severity and a recommended course of action in response to each event are also provided.

[Appendix C, *Restore Management Server*](#) - This appendix provides the instructions to restore all required switch applications to the management server in case of a hard drive failure.

[Appendix D, *Consolidating Management Servers*](#) - This appendix provides the instructions consolidate operation and network addressing of multiple management servers.

An [Index](#) is also provided.

Related Publications

Other publications that provide additional information about the switch include:

- *McDATA Products in a SAN Environment - Planning Manual* (620-000124).

- *McDATA Sphereon 4500 Fabric Switch Element Manager User Manual* (620-000175).
- *SANavigator Software Release 4.0 User Manual* (621-000013).
- *EFC Manager Software Release 8.0 User Manual* (620-000170).
- *McDATA SANpilot User Manual* (620-000160).
- *McDATA SNMP Support Manual* (620-000131).
- *McDATA E/OS Command Line Interface User Manual* (620-000134).
- *McDATA Sphereon 4300 and 4500 Switch Rack-Mount Kit Installation Instructions* (958-000316).
- *McDATA EFCM Lite Installation Instructions* (958-000171).
- *1U Server Rack-Mount Kit Installation Instructions* (958-000310).
- *McDATA FC-512 Fabriccenter Equipment Cabinet Installation and Service Manual* (620-000100).

Ordering Printed Manuals

To order a paper copy of this manual, submit a purchase order as described in *Ordering McDATA Documentation Instructions*, which is found on McDATA's web site, <http://www.mcdata.com>. To obtain documentation CD-ROMs, contact your sales representative.

Where to Get Help

For technical support, contact the McDATA Solution Center. The center provides a single point of contact for assistance, and is staffed 24 hours a day, seven days a week, including holidays. Contact the center at the phone number, fax number, or e-mail address listed below. Please have the product serial number (printed on the service label attached to the switch) available.

Phone: (800) 752-4572 or (720) 566-3910

Fax: (720) 566-3851

E-mail: support@mcdata.com

For technical support for the SANavigator[®] application, contact the SANavigator Solution Center at the phone number or e-mail address listed below.

Phone: (877) 948-4448

E-mail: support@sanavigator.com

**Forwarding
Publication
Comments**

We welcome comments about this publication. Please send comments to the McDATA Solution Center by telephone, fax, or e-mail. The numbers and e-mail address are listed above. Please identify the manual, page numbers, and details.

Trademarks

The following terms, indicated by a registered trademark symbol (®) or trademark symbol (™) on first use in this publication, are trademarks of McDATA Corporation or SANavigator, Inc. in the United States or other countries or both:

Registered Trademarks

McDATA®

Fabriccenter®

OPENready®

SANavigator®

Trademarks

Sphereon™

Networking the world's
business data™

OPENconnectors™

SANpilot™

SANtegrity™

EON™

All other trademarked terms, indicated by a registered trademark symbol (®) or trademark symbol (™) on first use in this publication, are trademarks of their respective owners in the United States or other countries or both.

**Laser Compliance
Statement**



Laser transceivers for the switch are tested and certified in the United States to conform to Title 21 of the Code of Federal Regulations (CFR), Subchapter J, Parts 1040.10 and 1040.11 for Class 1 laser products. Elsewhere, the transceivers are tested and certified to be compliant with International Electrotechnical Commission IEC825-1 and European Norm EN60825-1 and EN60825-2 regulations for Class 1 laser products. Class 1 laser products are not considered hazardous. The transceivers are designed such that there is never human access to laser radiation above a Class 1 level during normal operation or prescribed maintenance conditions.

**Federal
Communications
Commission (FCC)
Statement**

The switch generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with instructions provided, may cause interference to radio communications. The product was tested and found to comply with the limits for Class A computing devices pursuant to Subpart B of Part 15 of the FCC Rules, which are designed to provide reasonable protection against such interference in a commercial environment. Operation of the product

in a residential area is likely to cause interference in which case the user, at his or her own expense, will take whatever measures are required to correct the interference. Any modifications or changes made to the product without explicit approval from McDATA, by means of a written endorsement or through published literature, will invalidate the service contract and void the warranty agreement with McDATA.

Chinese National Standards Mark

The Chinese National Standards (CNS) mark illustrated below indicates switch compliance with Taiwanese Bureau of Standards, Metrology, and Inspection (BSMI) regulatory requirements.

警告使用者:

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

European Union Conformity Declarations for Information Technology Equipment

The switch meets the following regulatory requirements as set forth by European Norms (ENs) and relevant International Electrotechnical Commission (IEC) standards for commercial and light industrial information technology equipment (ITE).

- **EN55022: 1998; EN55024: 1997, +A1: 1998:** ITE-generic radio frequency interference (RFI) emission standard for domestic, commercial, and light industrial environments.
- **EN60950:** ITE-generic electrical and fire safety standard for domestic, commercial, and light industrial environments.

European Union Directives

The European Union (EU) Council has implemented a series of directives that define product safety standards for all EU member countries. The following directives apply to the switch:

- The product conforms with all protection requirements of EU directive 89/336/EEC (EMC Directive) in accordance with of the laws of the member countries relating to electromagnetic compatibility (EMC), emissions, and immunity.
- The product conforms with all protection requirements of EU directive 73/23/EEC (Low Voltage Directive) in accordance with of the laws of the member countries relating to electrical safety.

- The product conforms with all protection requirements of EU directive 93/68/EEC (Machinery Directive) in accordance with of the laws of the member countries relating to safe electrical and mechanical operation of the equipment.

McDATA does not accept responsibility for any failure to satisfy the protection requirements of any of these directives resulting from a non-recommended or non-authorized modification to a switch.

Danger and Attention Statements

The following **DANGER** statements appear in this publication and describe safety practices that must be observed while installing or servicing the switch. A **DANGER** statement provides essential information or instructions for which disregard or noncompliance may result in death or severe personal injury. Each **DANGER** statement appears in English, followed by translations to:

- Chinese (simplified - People's Republic of China).
- Chinese (traditional - Taiwan).
- French (European).
- German.
- Hebrew.
- Italian.
- Portuguese.
- Spanish (European).
- Spanish (Latin American).



DANGER

Use the supplied power cords. Ensure the facility power receptacle is the correct type, supplies the required voltage, and is properly grounded.



危險

使用所提供的电源线。确保使用正确型号的设备电源插座，提供必需的电压并且正确接地。



危險

使用隨附的電源線，確定使用正確類型的設備電源插座，提供必需的電壓，並且正確接地。



DANGER

Utiliser les câbles d'alimentation fournis. S'assurer que la prise de courant du local est du type correct, délivre la tension requise et est correctement raccordée à la terre.



GEFAHR

Die mitgelieferten Netzkabel verwenden. Sicherstellen, dass die verwendete Netzsteckdose dem vorgeschriebenen Typ entspricht, die erforderliche Spannung liefert und einwandfrei geerdet ist.

סכנה



השתמש בכבלי החשמל הנלווים. וודא כי כלי הקיבול לחשמל של המתקן הוא מהסוג הנכון, מספק את המתח הדרוש, ומוארק כהלכה.



PERICOLO

Usare il cavo di alimentazione in dotazione. Assicurarsi che la presa di corrente a disposizione sia del tipo corretto, eroghi la tensione richiesta e sia dotata di messa a terra idonea.



PERIGO

Use os cordões elétricos fornecidos. Certifique-se de que o tipo de receptor de energia da facilidade é apropriado, fornece a voltagem necessária, e está corretamente aterrado.



PELIGRO

Utilice los cables de alimentación proporcionados. Asegúrese que el receptáculo tomacorriente para la instalación sea el tipo correcto, suministre el voltaje necesario, y que esté apropiadamente puesto a tierra.



PELIGRO

Utilice los cables de alimentación proporcionados. Asegúrese que el receptáculo tomacorriente para la instalación sea del tipo correcto, suministre el voltaje necesario, y que esté apropiadamente conectado a tierra.



DANGER

Disconnect the power cords.



危険

拔除电源线。



危険

拔除電源線。



DANGER

Débrancher les câbles d'alimentation.



GEFAHR

Netzkabel abziehen.



סכנה

נתק את כבלי החשמל.



PERICOLO

Scollegare tutti i cavi di alimentazione.



PERIGO

Disconecte os cordões elétricos.



PELIGRO

Desconecte los cables de alimentación.



PELIGRO

Desconecte los cables de alimentación.

The following **ATTENTION** statements appear in this publication and describe practices that must be observed while installing or servicing the switch. An **ATTENTION** statement provides essential information or instructions for which disregard or noncompliance may result in equipment damage or loss of data.

ATTENTION ! Prior to servicing a product, management server, or customer-supplied server, determine the Ethernet LAN configuration. Installation of products and servers on a public customer intranet can complicate problem determination and fault isolation.

ATTENTION ! Activating a preferred path can result in receipt of out-of-order frames if the preferred path differs from the current path, if input and output (I/O) is active from the source port, and if congestions is present on the current path.

ATTENTION ! Do not remove a power supply unless a replacement FRU is immediately available. To avoid product overheating, a removed power supply must be replaced within five minutes.

ATTENTION ! A reset should only be performed if a CTP card failure is indicated. Do not reset a managed product unless directed to do so by a procedural step or the next level of support.

ATTENTION ! This procedure deletes all data from the C: hard drive partition.

ATTENTION ! Contents of the data directory are backed up to the management server's CD-RW drive when directory contents change. To ensure trouble-free backups, always leave a CD in the drive. Ensure data is not being written to or read from the CD-RW drive before removing the CD. Removing the CD during a backup or restore operation can corrupt data.

General Precautions

When installing or servicing the switch, follow these practices:

- Always use correct tools.
- Always use correct replacement parts.
- Keep all paperwork up to date, complete, and accurate.

ESD Precautions

All electrostatic discharge (ESD) sensitive components and FRUs in the switch are enclosed and shielded. ESD procedures are not required when working with the switch.

The McDATA® Sphereon™ 4500 Fabric Switch provides up to 24 ports of low-cost and high-performance dynamic Fibre Channel connectivity for switched fabric devices or arbitrated loop devices. This function allows low-cost, low-bandwidth workgroup (edge) devices to communicate with mainframe servers, mass storage devices, or other peripherals, and ultimately be incorporated into an enterprise storage area network (SAN) environment.

This chapter describes the switch and switch management through the SANpilot™ interface or the optional rack-mount management server. The chapter specifically describes:

- The switch, including field-replaceable units (FRUs), controls, connectors, and indicators, and switch specifications.
- Maintenance approach.
- Switch management through the SANpilot interface, rack-mount management server, or a remote workstation.
- Error detection, reporting, and serviceability features.
- Software diagnostic features.
- Tools and test equipment.

Switch Description

The Sphereon 4500 Switch provides Fibre Channel connectivity through 24 generic mixed ports (GX_Ports). Switch ports operate at either 1.0625 or 2.125 gigabits per second (Gbps), and can be configured as:

- Fabric ports (F_Ports) to provide direct connectivity for up to 24 switched fabric devices.
- Fabric loop ports (FL_Ports) to provide arbitrated loop connectivity and fabric attachment for FC-AL devices. Each FL_Port can theoretically support the connection of 126 FC-AL devices.
- Expansion ports (E_Ports) to provide interswitch link (ISL) connectivity to fabric directors and switches.

The switch can be installed on a table or desk top, mounted in a McDATA FC-512 Fabriccenter[®] equipment cabinet, or mounted in any standard 19-inch equipment rack. [Figure 1-1](#) illustrates the switch.



Figure 1-1 Sphereon 4500 Switch

Administrators or operators with a browser-capable PC and an Internet connection monitor and manage the switch through the SANpilot interface. The SANpilot interface manages only a single switch, and provides a graphical user interface (GUI) that supports product configuration, statistics monitoring, and basic operation. The SANpilot interface is opened from a standard web browser running Netscape Navigator[®] 4.6 or higher or Microsoft[®] Internet Explorer 4.0 or higher. At the browser, enter the Internet Protocol (IP) address of the switch as the Internet uniform resource locator (URL). When prompted at a login screen, enter a user name and password.

As an option, the switch can be managed through a one unit (1U) high, rack-mount management server running a Java™-based SAN management application (SANavigator® 4.0 or Enterprise Fabric Connectivity Manager (EFCM) 8.0) and the Sphereon 4500 Element Manager application.

Multiple switches and the server communicate on a local area network (LAN) through one or more 10/100 Base-T Ethernet hubs. One or more 24-port Ethernet hubs are optional and can be ordered with the switch. Up to three hubs are daisy-chained as required to provide additional Ethernet connections as more switches (or other managed products) are installed on a network.

Field-Replaceable Units

The switch provides a modular design that enables quick removal and replacement of FRUs, including small form factor pluggable (SFP) optical transceivers and power supply assemblies with internal cooling fans. [Figure 1-2](#) illustrates the front of the switch. SFP transceivers are the only FRUs accessed from the front. The figure also shows front-panel controls, connectors, and indicators.

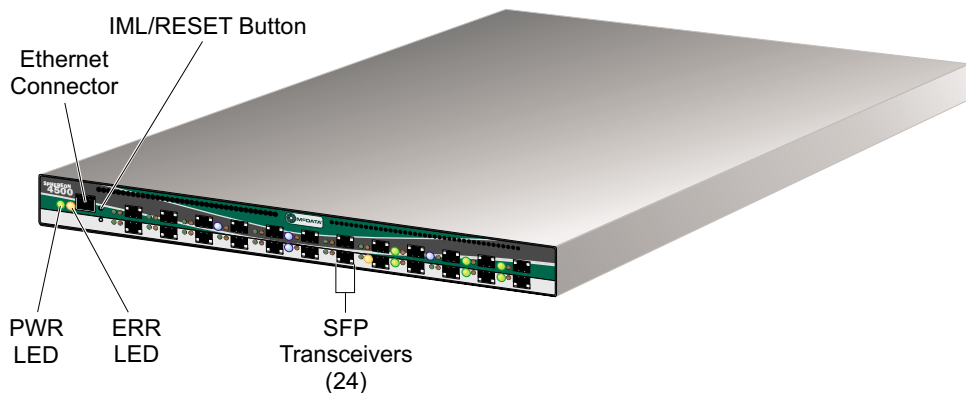


Figure 1-2 Sphereon 4500 Switch (Front View)

[Figure 1-3](#) on page 1-4 illustrates the rear of the switch. Power supply assemblies with internal cooling fans are the only FRUs accessed from the rear. The figure also shows the maintenance port.

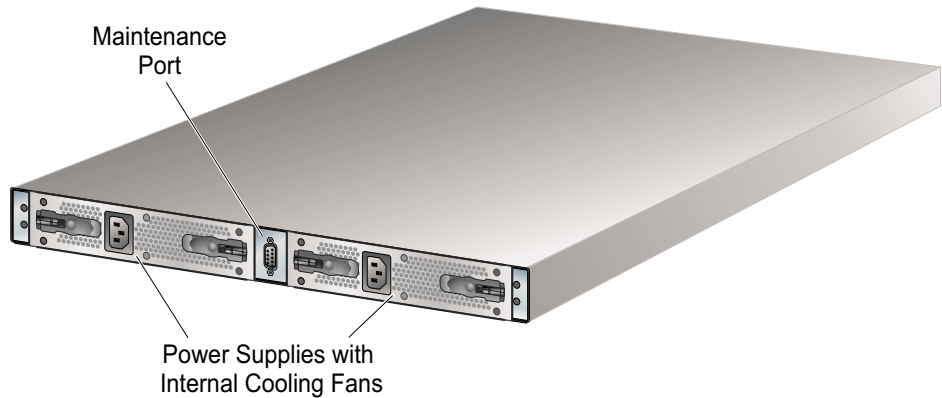


Figure 1-3 Sphereon 4500 Switch (Rear View)

SFP Transceiver

Singlemode or multimode fiber-optic cables attach to switch ports through SFP transceivers. The fiber-optic transceivers provide duplex LC[®] connectors, and can be detached from switch ports (through a 10-pin interface) for easy replacement. The following fiber-optic transceiver types are available:

- **Shortwave laser (1.0625 Gbps)** - Shortwave laser transceivers provide connections for transferring 1.0625 Gbps data over short distances as follows:
 - Up to 500 meters through 50-micron multimode fiber.
 - Up to 300 meters through 62.5-micron multimode fiber.
- **Shortwave laser (2.125 Gbps)** - Shortwave laser transceivers provide connections for transferring 2.125 Gbps data over short distances as follows:
 - Up to 300 meters through 50-micron multimode fiber.
 - Up to 150 meters through 62.5-micron multimode fiber.
- **Longwave laser (1.0625 Gbps)** - Longwave laser transceivers provide connections for transferring 1.0625 Gbps data up to 10 kilometers through 9-micron singlemode fiber.

- **Longwave laser (2.125 Gbps)** - Longwave laser transceivers provide connections for transferring 2.125 Gbps data up to 10 kilometers through 9-micron singlemode fiber.
- **Extended longwave laser (2.125 Gbps)** - Two types of extended longwave laser transceivers provide connections for transferring 2.125 Gbps data up to 20 kilometers or 35 kilometers through 9-micron singlemode fiber.

Power Supply Assembly

The switch contains two power supply assemblies with internal cooling fans. The redundant, load-sharing power supply assemblies step down and rectify facility input power to provide 3.3 volts direct current (VDC), 5 VDC, and 12 VDC to the control processor (CTP) card. The power supplies also provide input filtering, overvoltage protection, and overcurrent protection.

Either power supply can be replaced while the switch is operational. Each power supply has a separate connection to the CTP card to allow for independent AC power sources. The power supplies are input rated at 100 to 240 volts alternating current (VAC).

Three cooling fans integrated in each power supply assembly (six fans total) provide cooling for the power supplies and CTP card, as well as redundancy for continued operation if a single fan fails. Fans are removed and replaced as part of the integrated power supply.

Controls, Connectors, and Indicators

Controls, connectors, and indicators for the switch include the:

- Combined initial machine load and reset (**IML/RESET**) button.
- Ethernet LAN connector.
- Green power (**PWR**) and amber system error (**ERR**) light-emitting diodes (LEDs).
- Green, blue, and amber status LEDs associated with FRUs.
- RS-232 maintenance port.

IML/Reset Button

When the **IML/RESET** button (Figure 1-2 on page 1-3) is pressed, held for three seconds, and released, the switch performs an IML that reloads the firmware from FLASH memory. This operation is not disruptive to Fibre Channel traffic. If the button is held for more than three seconds, the **ERR** LED blinks at twice the unit beaoning rate.

When the **IML/RESET** button is pressed and held for ten seconds, the switch performs a reset. After three seconds, the **ERR** LED blinks at twice the unit beaoning rate. A reset is disruptive and resets the:

- Microprocessor and functional logic for the CTP card and reloads the firmware from FLASH memory.
- Ethernet LAN interface, causing the connection to the management server to drop momentarily until the connection automatically recovers.
- Ports, causing all Fibre Channel connections to drop momentarily until the connections automatically recover. This causes attached devices to log out and log back in, therefore data frames lost during switch reset must be retransmitted.

A reset should only be performed if a CTP card failure is indicated. As a precaution, the **IML/RESET** button is flush mounted to protect against inadvertent activation.

Ethernet LAN Connector

The front panel provides a 10/100 megabit per second (Mbps) RJ-45 twisted-pair connector (Figure 1-2 on page 1-3) that attaches to an Ethernet LAN to provide communication with the management server or a simple network management protocol (SNMP) management workstation. The connector provides two green LEDs. The left LED illuminates to indicate LAN operation at 10 Mbps, while the right LED illuminates to indicate LAN operation at 100 Mbps.

Power and System Error LEDs

The **PWR** LED (Figure 1-2 on page 1-3) illuminates when the switch is connected to facility AC power and is operational (the switch does not have a power switch). If the LED extinguishes, a facility power source, power cord, or power distribution failure is indicated.

The **ERR** LED (Figure 1-2 on page 1-3) illuminates when the switch detects an event requiring immediate operator attention, such as a FRU failure. The LED remains illuminated as long as an event is active. The LED extinguishes when *Clear System Error Light* is selected from the SANpilot interface or Element Manager application.

The LED blinks if unit beaconing is enabled. An illuminated LED (indicating a failure) takes precedence over unit beaconing. The LED also blinks (at twice the beaconing rate) when the **IML/RESET** button is pressed and held for more than three seconds.

FRU Status LEDs

Amber and green/blue LEDs associated with switch FRUs provide status information as follows:

- **Fibre Channel ports** - LEDs to the left of each port ([Figure 1-2](#) on page 1-3) illuminate, extinguish, or blink to indicate port status and port speed. The amber LED illuminates if the port fails. The green/blue LED illuminates green to indicate 1.0625 Gbps port operation. The green/blue LED illuminates blue to indicate 2.125 Gbps port operation.
- **Power supply assembly** - An amber LED on each assembly ([Figure 1-3](#) on page 1-4) illuminates if the FRU fails.

Maintenance Port

The rear panel provides a 9-pin DSUB maintenance port ([Figure 1-3](#) on page 1-4) that provides a connection for a local terminal or dial-in connection for a remote terminal. Although the port is typically used only by authorized maintenance personnel, operations personnel can use the port to configure switch network addresses.

Switch Specifications

This section lists physical characteristics, storage and shipping environment, operating environment, and service clearances for the Sphereon 4500 Switch.

Physical Characteristics

Dimensions:

Height: 4.1 centimeters (1.6 inches) or 1 rack unit

Width: 43.7 centimeters (17.2 inches)

Depth: 47.3 centimeters (18.6 inches)

Weight: 8.6 kilograms (19.0 pounds)

Power requirements:

Input voltage: 100 to 240 VAC

Storage and Shipping Environment

Input frequency: 47 to 63 Hz

Plan for single phase or phase-to-phase connections and 5-ampere dedicated service

Heat dissipation:

49 watts (167 BTUs/hr)

Cooling airflow clearances (switch chassis):

Right and left side: 1.3 centimeters (0.5 inches)

Front and rear: 7.6 centimeters (3.0 inches)

Top and bottom: No clearance required

Shock and vibration tolerance:

60 Gs for 10 milliseconds without nonrecoverable errors

Acoustical noise:

64 dB "A" scale

Inclination:

10⁰ maximum

Protective packaging must be provided to protect the switch under all shipping methods (domestic and international).

Shipping temperature:

-40⁰ F to 140⁰ F (-40⁰ C to 60⁰ C)

Storage temperature:

34⁰ F to 140⁰ F (1⁰ C to 60⁰ C)

Shipping relative humidity:

5% to 100%

Storage relative humidity:

5% to 80%

Maximum wet-bulb temperature:

84⁰ F (29⁰ C)

Altitude:

40,000 feet (12,192 meters)

Operating Environment**Temperature:**

40⁰ F to 104⁰ F (4⁰ C to 40⁰ C)

Relative humidity:

8% to 80%

Maximum wet-bulb temperature:

81⁰ F (27⁰ C)

Altitude:

10,000 feet (3,048 meters)

Maintenance Approach

Whenever possible, the switch maintenance approach instructs service personnel to perform fault isolation and repair procedures without degrading or interrupting operation of the switch, attached devices, or associated applications. Switch fault isolation begins when one or more of the following occur:

- System event information displays at a browser-capable PC communicating with the switch through the SANpilot interface.
- System event information displays at a LAN-connected PC or workstation communicating with the rack-mount management server running a SAN management application.
- LEDs on the switch front panel or FRUs illuminate to indicate a hardware malfunction.
- An unsolicited SNMP trap message is received at a management workstation, indicating an operational state change or failure.
- Notification of a significant system event is received at a designated support center through an E-mail message or the call-home feature.

System events can be related to a:

- Switch or management server failure (hardware or software).
- Ethernet LAN communication failure between the switch and management server.
- Link failure between a port and attached device.
- ISL failure or segmentation of an E_Port.

Fault isolation and service procedures vary depending on the system event information provided. Fault isolation and related service information is provided through maintenance analysis procedures (MAPs) documented in Chapter 3. MAPs consist of step-by-step procedures that prompt service personnel for information or describe a specific action to be performed. MAPs provide information to interpret system event information, isolate a switch failure to a single FRU, remove and replace the failed FRU, and verify switch operation. The fault isolation process normally begins with [MAP 0000: Start MAP](#) on page 3-6.

Ensure the correct switch is selected for service by enabling unit beaconing at the failed switch. The amber system error (**ERR**) LED on the switch front panel blinks when beaconing is enabled. Instructions to enable beaconing are incorporated into MAP steps.

Switch Management

The switch is managed and controlled through a:

- Customer-supplied PC platform with an Internet connection to the SANpilot interface on the switch. Using this graphical user interface (GUI), operators can quickly view switch status.

The interface allows service personnel to perform configuration tasks, view system alerts and related log information, and monitor switch status, port status, and performance. FRU status and system alert information are highly visible.

- Optional 1U management server (running a SAN management application) that provides a central point of control for up to 48 switches or managed products.

The management server is delivered with a *server* and *client* SAN management application (SANavigator 4.0 or EFCM 8.0) and the Sphereon 4500 Element Manager application installed. A customer-supplied PC or workstation (with *client* applications installed) communicates with the server through a corporate intranet.

- Customer-supplied PC or UNIX-based platform with the *server* and *client* SANavigator and Sphereon 4500 Element Manager applications installed.

SANpilot Interface

With switch firmware Version 4.0 (or later) installed, administrators or operators with a browser-capable PC and an Internet connection can monitor and manage the switch through the SANpilot interface. The application provides a GUI that supports switch configuration, operation, performance monitoring, maintenance and diagnostic functions.

The SANpilot interface is opened from a standard web browser running Netscape Navigator® Version 4.6 (or higher) or Microsoft Internet Explorer Version 4.0 (or higher). At the browser, enter the IP address of the switch as the Internet uniform resource locator (URL).

Management Server

The management server is a 1U, rack-mount unit that provides a central point of control for up to 48 connected switches or other managed products. Server applications are accessed through a LAN-attached PC or workstation with client software installed. [Figure 1-4](#) illustrates the server with attached liquid crystal display (LCD) panel.



Figure 1-4 Management Server

The server is rack mounted in the McDATA-supplied FC-512 Fabriccenter equipment cabinet. A SANpilot interface or management server is required to install, configure, and manage the switch.

The server provides two auto-detecting 10/100 Mbps Ethernet LAN connectors (RJ-45 adapters). The first adapter (LAN 1) attaches (optionally) to a public customer intranet to allow access from remote user workstations. The second adapter (LAN 2) attaches to a private LAN segment containing switches or managed products.

Management Server Specifications

The following list summarizes hardware specifications for the rack-mount management server platform. Current platforms may ship with more enhanced hardware, such as a faster processor, additional random-access memory (RAM), or a higher-capacity hard drive.

**Ethernet Hub
(Optional)**

- 1U rack-mount server running the Intel® Pentium® 4 processor with an 1,800 megahertz (MHz) or greater clock speed, Microsoft Windows® 2000 Professional operating system, and power cord.
- TightVNC™ Viewer Version 1.2.7 client-server software control package that provides remote network access (through a standard web browser) to the management server desktop.
- 1,024 megabyte (MB) or greater RAM.
- 40 gigabyte (GB) or greater internal hard drive.
- 1.44 MB 3.5-inch slim-type disk drive and slim-type compact disk-rewritable (CD-RW) drive.
- 56K internal modem.
- Two 10/100 Mbps Ethernet adapters with RJ-45 connectors.

The management server and managed switches connect through a 10/100 Base-T Ethernet hub. [Figure 1-5](#) illustrates the 24-port hub.

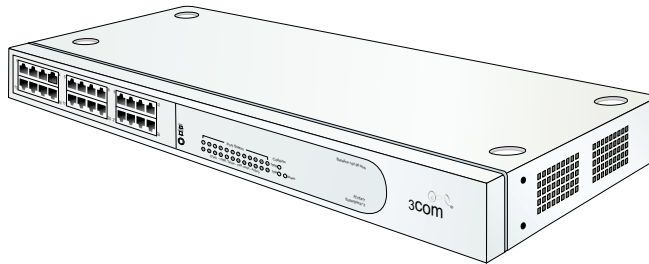


Figure 1-5 24-Port Ethernet Hub

Hubs can be daisy-chained to provide additional connections as more switches (or other McDATA managed products) are installed on a network. Multiple hubs are daisy-chained by attaching RJ-45 Ethernet patch cables and configuring each hub through a medium-dependent interface (MDI) switch.

**Client PC or
Workstation**

Using a standard web browser, the client SAN management and Sphereon 4500 Element Manager applications can be downloaded and installed on PCs or workstations that are LAN-attached to the management server. Operators at these platforms can manage and monitor switches controlled by the server. A maximum of 25 concurrent users can log in to the management server. Each client

must have access to the LAN segment on which the management server is installed. Switch administrative functions are accessed through the LAN and server. The LAN interface can be:

- Part of the dedicated 10/100 Mbps segment (LAN 2) that provides access to managed switches. This switch-to-server connection is part of the required equipment installation. Connection of client PCs and workstations can be through the McDATA Ethernet hub or through the customer intranet. A network configuration using the customer intranet and one Ethernet connection through the server is shown in [Figure 1-6](#).

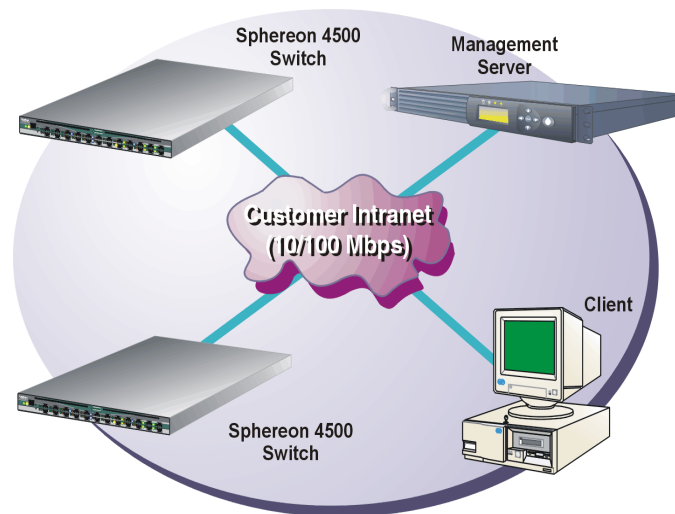


Figure 1-6 Typical Network Configuration (One Ethernet Connection)

If only one management server connection is used and this connection is provided through the customer intranet, functions provided by the server are available to all users. The purpose for dual LAN connections is to provide a dedicated LAN segment that isolates the server and managed switches from unauthorized users.

NOTE: Both Ethernet adapters in the management server provide auto-detecting 10/100 Mbps connections. The dedicated LAN segment that connects the server to managed switches and the optional customer intranet operate at either ten or 100 Mbps.

- Part of a second management server interface (LAN 1) that connects to a customer intranet and allows operation of the Sphereon 4500 Element Manager application from client PCs or workstations. Connection to this LAN segment is optional and depends on customer requirements. A network configuration using both Ethernet connections is shown in [Figure 1-7](#).

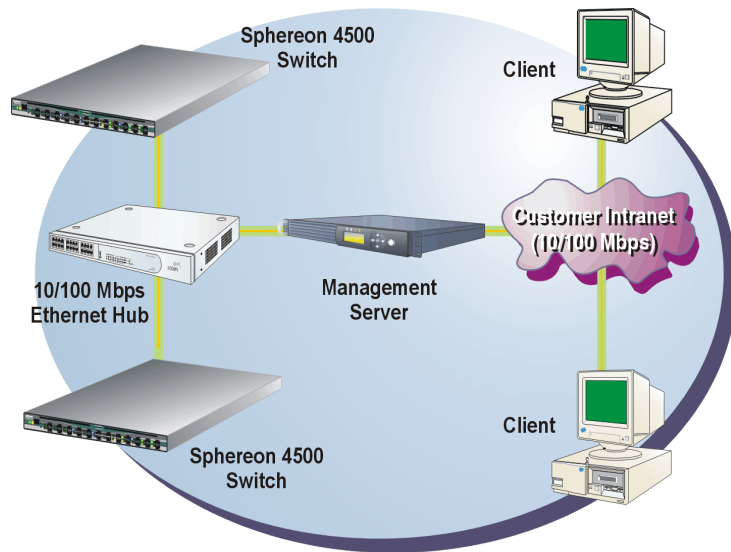


Figure 1-7 Typical Network Configuration (Two Ethernet Connections)

ATTENTION ! Prior to servicing a product, management server, or customer-supplied server, determine the Ethernet LAN configuration. Installation of products and servers on a public customer intranet can complicate problem determination and fault isolation.

Minimum Client Specifications

Client SAN management and Element Manager applications download and install to remote workstations (from the 1U management server) using a standard web browser. The applications operate on platforms that meet the following minimum system requirements:

- Desktop or notebook PC with color monitor, keyboard, and mouse, using an Intel Pentium III processor with a 700 MHz or greater clock speed, and using the Microsoft Windows 2000 (with service pack 4), Windows NT 4.0 (with service pack 6a), or Windows 2003 operating system.

- Unix workstation with color monitor, keyboard, and mouse, using a:
 - Linux-based system using an Intel Pentium III processor with a 1 gigahertz (GHz) or greater clock speed, using the Red Hat® 7.3 or higher operating system.
 - Hewlett-Packard® PA-RISC® processor with a 400 MHz or greater clock speed, using the HP-UX® 11 or higher operating system.
 - Sun® Microsystems UltraSPARC™ Ili or later processor, using Solaris™ Version 7.0 or higher operating system.
 - IBM POWER3-II™ microprocessor with a 333 MHz or greater clock speed, using the AIX Version 4.3.3 or higher operating system.
- At least 150 MB (Windows-based) or 350 MB (Unix-based) available on the internal hard drive.
- 512 MB or greater RAM.
- Video card supporting 256 colors at 800 x 600 pixel resolution.
- Ethernet network adapter.
- Java-enabled Internet browser, such as Microsoft Internet Explorer (Version 4.0 or later) or Netscape Navigator (Version 4.6 or later).

Error-Detection, Reporting, and Serviceability Features

The switch provides the following error detection, reporting, and serviceability features:

- LEDs on switch FRUs and adjacent to Fibre Channel ports that provide visual indicators of hardware status or malfunctions.
- Redundant FRUs (SFP transceivers and integrated cooling fan and power supply assemblies) that are removed or replaced without disrupting switch or Fibre Channel link operation.
- A modular design that enables quick removal and replacement of FRUs without the use of tools or equipment.

- System alerts and logs that display switch, Ethernet link, and Fibre Channel link status at the SANpilot interface, client communicating with the management server, or customer-supplied server (running a SAN management application).
- Diagnostic software that performs power-on self-tests (POSTs) and port diagnostics (loopback tests).
- An RS-232 maintenance port at the rear of the switch (port access is password protected) that enables installation or service personnel to change the switch's IP address, subnet mask, and gateway address.

These parameters can also be changed through a Telnet session, access for which is provided through a local or remote PC with an Internet connection to the switch.

- Data collection through the SANpilot interface or Element Manager application to help isolate system problems. The data includes a memory dump file and audit, hardware, and engineering logs.
- Beaconing to assist service personnel in locating a specific port or switch. When port beaconing is enabled, the amber LED associated with the port flashes. When unit beaconing is enabled, the system error indicator on the front panel flashes. Beaconing does not affect port or switch operation.
- An internal modem for use by support personnel to dial-in to the management server (optional) for event notification and to perform remote diagnostics.
- Automatic notification of significant system events (to support personnel or administrators) through e-mail messages or the call-home feature.

NOTE: The call-home feature is not available through the SANpilot interface. The call-home feature may not be available if the EFCM 8.0 Lite application is installed on a customer-supplied platform.

- SNMP management using the Fibre Channel Fabric Element MIB (Version 1.1), Transmission Control Protocol/Internet Protocol (TCP/IP) MIB-II definition (RFC 1157), or a product-specific private enterprise MIB that runs on the switch. Up to six authorized management workstations can be configured through the SANpilot interface or Element Manager application to receive unsolicited SNMP trap messages. The trap messages indicate product operational state changes and failure conditions.
- Optional SNMP management using the Fibre Alliance MIB (Version 3.1) that runs on the management server. Up to 12 authorized management workstations can be configured through the SAN management application to receive unsolicited SNMP trap messages. The trap messages indicate operational state changes and failure conditions.

Software Diagnostic Features

The switch provides the following diagnostic software features that aid in fault isolation and repair of problems:

- Switch FRUs provide on-board diagnostic and monitoring circuits that continuously report FRU status to the SANpilot interface and the SAN management and Element Manager applications. These applications provide system alerts and logs that display failure and diagnostic information.
- Unsolicited SNMP trap messages that indicate operational state changes or failures can be transmitted to up to 12 authorized management workstations.
- E-mail messages or call-home reports provide automatic notification of significant system events to designated support personnel or administrators.

NOTE: The call-home feature is not available through the SANpilot interface. The call-home feature may not be available if the EFCM 8.0 Lite application is installed on a customer-supplied platform.

SANpilot Interface

The SANpilot interface provides a GUI accessed through the Internet (locally or remotely) to manage, monitor, and isolate problems for the Sphereon 4500 Switch. When the interface opens, the default display is the *View* panel ([Figure 1-8](#) on page 1-18).

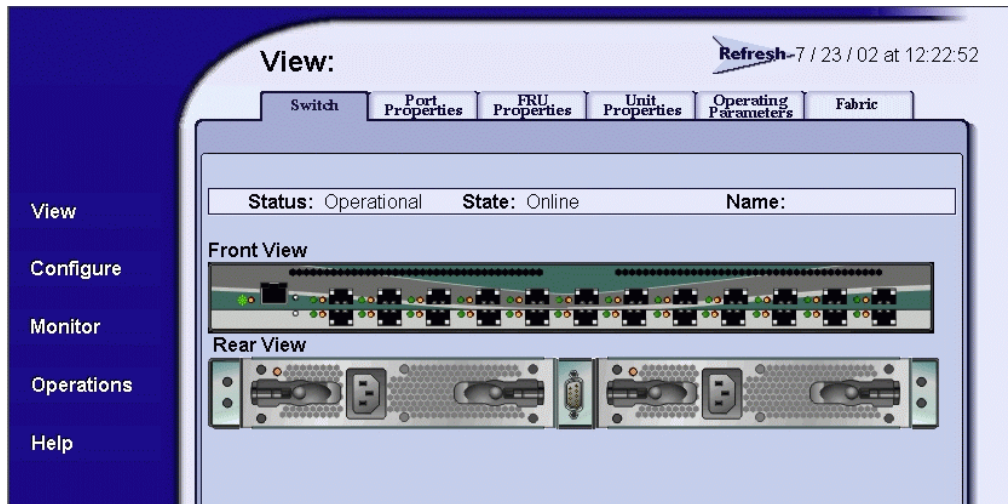


Figure 1-8 View Panel (SANpilot Interface)

Task selection tabs appear at the top of the panel, a graphical representation of the switch hardware (front and rear) appears at the right side of the panel, and menu selections (*View*, *Configure*, *Monitor*, *Operations*, and *Help*) appear at the left side of the panel. The task selection tabs allow personnel to perform switch-specific tasks, and are a function of the menu selected as follows:

- **View** - At the *View* panel, the *Switch* (default), *Port Properties*, *FRU Properties*, *Unit Properties*, *Operating Parameters*, and *Fabric* task selection tabs appear.
- **Configure** - At the *Configure* panel, the *Ports* (default), *Switch*, *Management*, *Zoning*, *Security*, and *Performance* task selection tabs appear.
- **Monitor** - At the *Monitor* panel, the *Port List* (default), *Port Stats*, *Log*, and *Node List* task selection tabs appear.
- **Operations** - At the *Operations* panel, the *Switch* (default), *Port*, *Maintenance*, and *Feature Installation* task selection tabs appear.
- **Help** - The *Help* selection opens online user documentation that supports the SANpilot interface.

Management Server

Optional SAN management (SANavigator 4.0 or EFCM 8.0) and Element Manager applications provide a GUI to manage, monitor, and isolate problems for multiple switches and multiswitch fabrics. The server and client applications operate on the management server, and a user interface is provided through an Ethernet LAN-attached PC or workstation running client-only applications.

SAN Management Application

The SAN management application opens automatically when the management server desktop is accessed, and the SANavigator or EFCM main window opens by default (Figure 1-9).

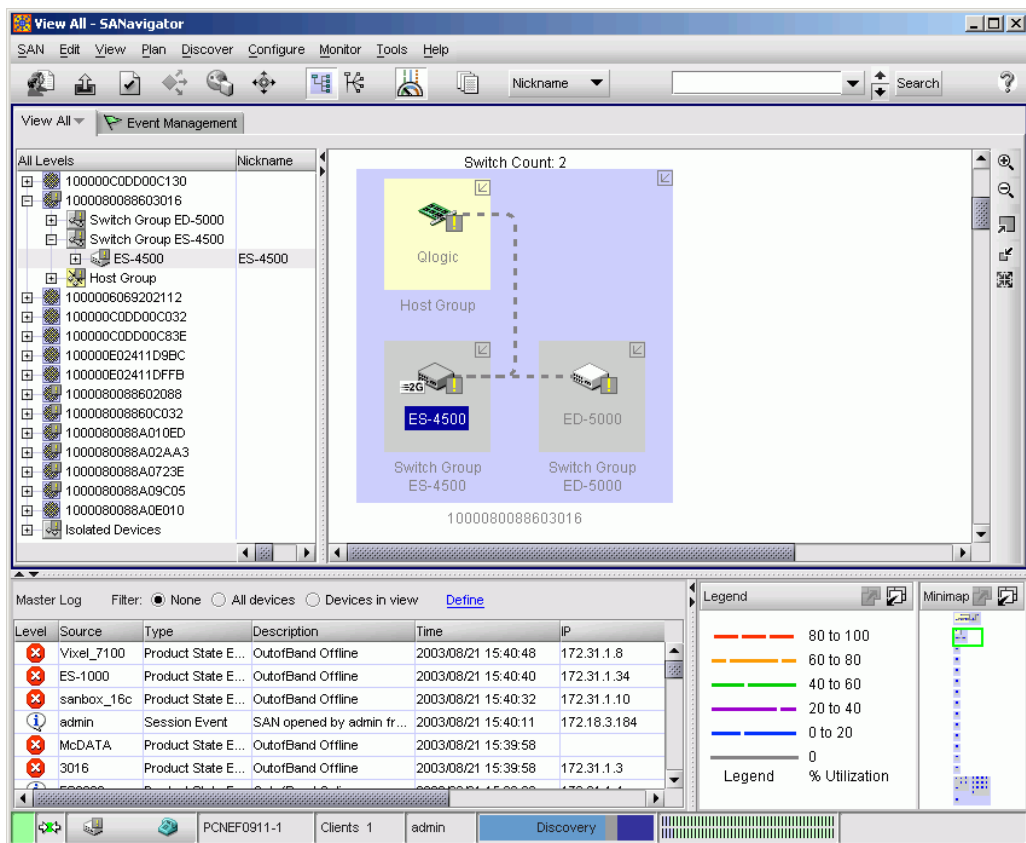


Figure 1-9 Main Window (SANavigator or EFCM)

The main window provides a:

- **Menu bar** - Commands at the top of the window provide drop-down menu selections to perform functions for SAN devices, including editing, viewing, planning, discovery, configuration, and monitoring.
- **Tool bar** - The tool bar (below the menu bar) provides button selections to perform SAN management tasks, including opening a SAN configuration, configuring users, setting up and starting the device discovery process, configuring zoning, displaying a SAN, displaying SAN utilization, and viewing reports.
- **View tab** - Select the *View* tab to display a product list and physical map of the discovered topology.
- **Product list** - When the *View* tab is selected, the product list at the left side of the window displays a list of discovered devices and associated properties.
- **Physical map** - When the *View* tab is selected, the physical map at the right side of the window depicts the SAN topology, discovered devices, and color-coded links.
- **Tool box** - The toolbox at the right side of the window provides button selections to change the discovered topology display, including zoom-in, zoom-out, expand, and collapse functions.
- **Master log** - The master log at the lower left corner of the window displays a list of informational, warning, or fatal events. The log also includes the event source, type, description, time, and IP address of the device generating the event.
- **Utilization legend** - The color-coded utilization legend explains percent utilization for links depicted on the physical map.
- **Minimap** - The minimap at the lower right corner of the window displays the entire SAN topology, and provides an aid to navigate the more detailed physical map.
- **Status bar** - The status bar at the bottom of the window displays connection status, client information, user level, and discovery status.

McDATA directors and switches, original equipment manufacturer (OEM) directors and switches, and other OEM devices display as icons in the SANavigator 4.0 main window. Only McDATA directors and switches (managed or unmanaged) display as icons in the EFCM 8.0 main window.

A label below each icon identifies the managed product. Additional information associated with each icon includes:

- **Data transmission rate** - 2.125 Gbps devices have a **2G** label.
- **Attention indicator** - A colored alert symbol adjacent to a product icon indicates the operational status of the product as follows:
 - Absence of an alert symbol indicates the product is fully operational.
 - A yellow triangle indicates a redundant component failure or degraded operational status.
 - A red diamond indicates a critical failure and the product is not operational.
 - A grey square with a yellow exclamation mark indicates the product status is unknown (network connection failure), or the product is offline.

For additional information about the SAN management applications, refer to the *SANavigator Software Release 4.0 User Manual* (621-000013) or the *EFC Manager Software Release 8.0 User Manual* (620-000170).

Element Manager Application

To open the Sphereon 4500 Element Manager application, right-click the product icon ([Figure 1-10](#)) at the SAN management application's physical map, then select the *Element Manager* option from the pop-up menu.



Figure 1-10 Sphereon 4500 Product Icon

When the Element Manager application opens, the last view (tab) accessed by a user opens by default. As an example, the *Hardware View* ([Figure 1-11](#) on page 1-22) is shown. A *Sphereon 4500 Status* table appears at the top of the window, and a graphical representation of the hardware (front and rear) appears in the center of the window.

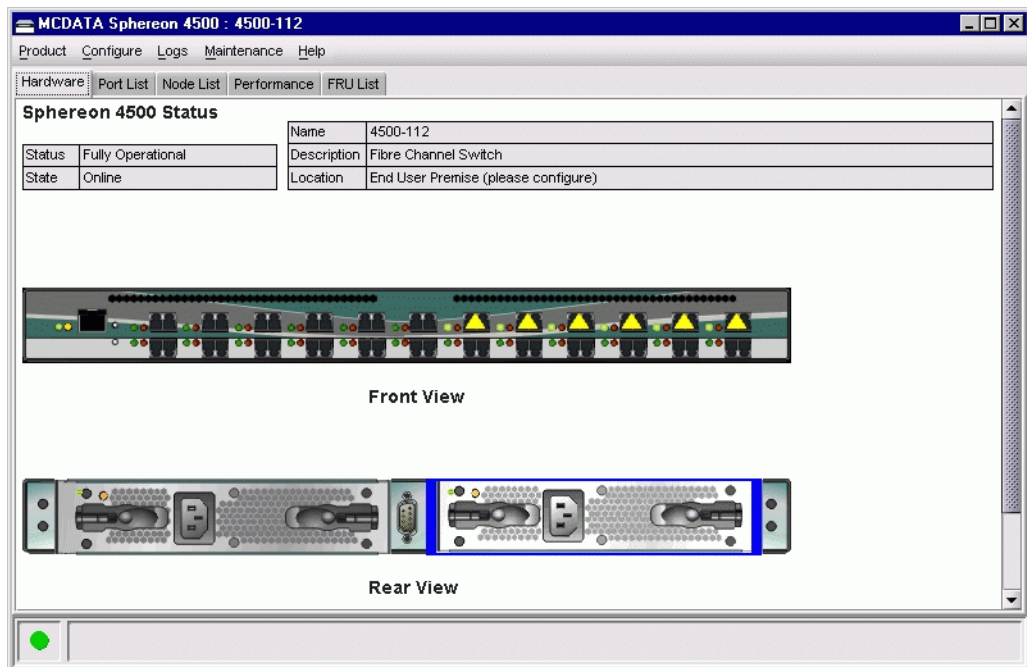


Figure 1-11 Hardware View

The graphical representation of the switch emulates the hardware configuration and operational status of the corresponding real switch. For example, if the switch is fully redundant and fully populated, this configuration is reflected in the *Hardware View*.

When the mouse cursor is moved over a graphical FRU, the FRU border highlights in blue and a pop-up identification label appears. Mouse selections (right or left click) open dialog boxes or menus that display FRU properties or allow users to perform operations and maintenance tasks. Colored symbols appear on the graphical FRUs to represent failed or degraded status. The LEDs also highlight to emulate real LED operation.

For a description of the Element Manager application, refer to the *McDATA Sphereon 4500 Fabric Switch Element Manager User Manual* (620-000175).

SNMP Trap Message Support

Unsolicited SNMP trap messages that indicate switch operational state changes or failure conditions can be customer-configured to be transmitted to up to 12 management workstations. If installed on a dedicated Ethernet LAN, the workstations communicate directly with each switch. If installed on a customer intranet, the workstations communicate with switches through the management server.

SNMP data and trap messages are defined in the Fibre Channel FE-MIB definition, a subset of the TCP/IP MIB-II definition (RFC 1157), and a custom, switch-specific MIB. Customers can install these MIBs (in standard ASN.1 format) on any SNMP management workstation.

Although SNMP trap messages are typically transmitted to customer personnel only, the messages may be provided to service personnel as initial notification of a switch problem or as information included in the fault isolation process. Generic SNMP traps include:

- **coldStart** - reports that the SNMP agent is reinitializing due to a switch reset.
- **warmStart** - reports that the SNMP agent is reinitializing due to a switch reset or initial program load (IPL).
- **authorizationFailure** - reports attempted access by an unauthorized SNMP manager. This trap is configurable and is disabled by default.

Switch-specific SNMP traps specified in the custom MIB include Fibre Channel port operational state changes and FRU operational state changes.

If authorized through the *Configure SNMP* dialog box in the Element Manager application, users at SNMP management workstations can modify MIB variables. Switch modifications performed through SNMP management work stations are recorded in the associated Sphereon 4500 audit log and are available through the Element Manager application. For additional information, refer to the *McDATA OPENconnectors SNMP Support Manual* (620-000131).

E-Mail and Call-Home Support

If E-mail notification and call-home support are configured for the switch as part of the customer support process, service personnel may be:

- Notified of a switch problem by E-mail message, either directly or through a system administrator at the customer site or call center.
- Assigned a service call from call center personnel upon receipt and confirmation of a switch call-home event.

NOTE: The call-home feature is not available through the SANpilot interface. The call-home feature may not be available if the EFCM 8.0 Lite application is installed on a customer-supplied platform.

Tools and Test Equipment

This section describes tools and test equipment that may be required to install, test, service, and verify operation of the switch and attached management server. These tools are supplied with the switch or must be supplied by service personnel.

Tools Supplied with the Switch

The following tools are supplied with the switch. Use of the tools may be required to perform one or more installation, test, service, or verification tasks.

- **Loopback plug** - An SFP multimode (shortwave laser) or singlemode (longwave laser) loopback plug ([Figure 1-12](#)) is required to perform port loopback diagnostic tests. One loopback plug is shipped with the switch, depending on the type of port transceivers installed. Both plugs are shipped if shortwave laser and longwave laser transceivers are installed.

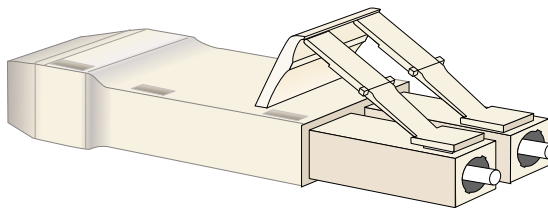


Figure 1-12 Loopback Plug

- **Fiber-optic protective plug** - For safety and port transceiver protection, fiber-optic protective plugs (Figure 1-13) must be inserted in all switch ports without fiber-optic cables attached. The switch is shipped with protective plugs installed in all ports.

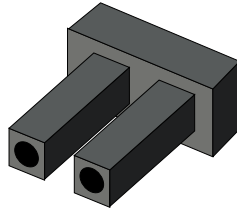


Figure 1-13 Fiber-Optic Protective Plug

- **Null modem cable** - An asynchronous RS-232 null modem cable (Figure 1-14) is required to configure switch network addresses and acquire event log information through the maintenance port. The cable has nine conductors and DB-9 male and female connectors.

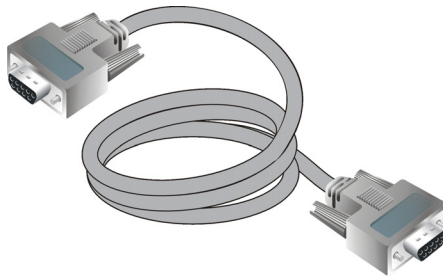


Figure 1-14 Null Modem Cable

Tools Supplied by Service Personnel

The following tools are expected to be supplied by service personnel performing switch installation or maintenance actions. Use of the tools may be required to perform one or more test, service, or verification tasks.

- **Scissors or pocket knife** - A sharp cutting edge (scissors or knife blade) may be required to cut the protective strapping when unpacking replacement FRUs.

- **Cross-tip (#2 Phillips) screwdriver** - The screwdriver is required to rack-mount the switch or to remove, replace, adjust or tighten various chassis or cabinet components.
- **T10 Torx® tool** - The tool is required to rack-mount the switch or to remove, replace, adjust or tighten various chassis or cabinet components.
- **Maintenance terminal (desktop or notebook PC)** - The PC is required to configure switch network addresses and acquire event log information through the maintenance port. The PC must have:
 - The Microsoft Windows 98, Windows 2000, Windows 2003, Windows XP, or Millennium Edition operating system installed.
 - RS-232 serial communication software (such as ProComm Plus™ or HyperTerminal) installed. HyperTerminal is provided with Windows operating systems.
- **Fiber-optic cleaning kit** - The kit contains tools and instructions to clean fiber-optic cable, connectors, loopback plugs, and protective plugs.

This chapter describes tasks to install, configure, and verify operation of the Sphereon 4500 Fabric Switch, SANpilot interface, and rack-mount management server. The switch can be installed on a table top, mounted in a McDATA FC-512 Fabriccenter equipment cabinet, or mounted in any standard 19-inch equipment rack.

Factory Defaults

[Table 2-1](#) lists factory-set defaults for the Sphereon 4500 Switch.

Table 2-1 Factory-Set Defaults (Sphereon 4500 Switch)

Item	Default
SANpilot interface user name (case sensitive)	Administrator
SANpilot interface password (case sensitive)	password
Customer-level password (maintenance port access)	password
Maintenance-level password (maintenance port access)	level-2
IP address	10.1.1.10
Subnet mask	255.0.0.0
Gateway address	0.0.0.0

[Table 2-2](#) on page 2-2 lists factory-set defaults for the one rack unit (1U) high, rack-mount management server.

Table 2-2 Factory-Set Defaults (Management Server)

Item		Default
Liquid crystal display (LCD) front panel		9999
Windows 2000 operating system user name (case sensitive)		Administrator
Windows 2000 operating system password (case sensitive)		password
SAN management application user name (case sensitive)		Administrator
SAN management application password (case sensitive)		password
LAN 1 (public interface)	IP address	192.168.0.1
	Subnet mask	255.0.0.0
	Gateway address	0.0.0.0
LAN 2 (private interface)	IP address	10.1.1.1
	Subnet mask	255.0.0.0
	Gateway address	0.0.0.0

Installation Options

The switch is installed in one of three configurations. The options are:

- **Table or desktop** - One or more switches, an optional management server, and an optional Ethernet hub are delivered and installed at the customer facility on a table or desktop. Ethernet cabling, distance, and local area network (LAN) addressing issues must be considered.
- **Fabriccenter equipment cabinet** - One or more switches, a rack-mount management server, and an Ethernet hub are delivered (cabled and installed) in a McDATA equipment cabinet. Ethernet cabling, distance, and LAN addressing issues must only be considered if multiple cabinets are daisy-chained.

- **Customer-supplied equipment rack** - One or more switches, an optional management server, and an optional Ethernet hub are delivered to the customer facility for installation in a customer-supplied equipment rack. Rack mount flanges and hardware are provided in the shipping containers. Ethernet cabling, distance, and LAN addressing issues must be considered.

Summary of Installation Tasks

[Table 2-3](#) summarizes installation tasks for the switch, optional management server, and optional Ethernet hub. The table describes each task, states if the task is optional, and lists the page reference.

Table 2-3 Installation Task Summary

Task Number and Description	Required or Optional	Page
<i>Task 1: Verify Installation Requirements.</i>	Required.	2-4
<i>Task 2: Unpack, Inspect, and Install the Ethernet Hub (Optional).</i>	Optional - perform this task only if the hub is required to connect the switch to the Internet (SANpilot interface) or to the management server.	2-5
<i>Task 3: Unpack, Inspect, and Install the Switch.</i>	Required.	2-10
<i>Task 4: Configure the Switch at the SANpilot Interface (Optional).</i>	Optional - perform this task if the switch is managed through the SANpilot interface.	2-13
<i>Task 5: Configure Switch Network Information (Optional).</i>	Configure if connecting multiple switches or if connecting a switch and management server to a public LAN.	2-41
<i>Task 6: Unpack, Inspect, and Install the Management Server.</i>	Required if the management server is installed.	2-47
<i>Task 7: Configure Server Password and Network Addresses.</i>	Required if the management server is installed.	2-51
<i>Task 8: Configure Management Server Information.</i>	Required if the management server is installed.	2-55
<i>Task 9: Configure Windows 2000 Users.</i>	Required if the management server is installed.	2-63
<i>Task 10: Set Management Server Date and Time.</i>	Required if the management server is installed.	2-69
<i>Task 11: Configure the Call-Home Feature (Optional).</i>	Optional - configure if the management server is installed, if specified by the customer, and if a telephone connection is provided.	2-71
<i>Task 12: Assign User Names and Passwords.</i>	Required if the management server is installed.	2-72

Table 2-3 Installation Task Summary (*continued*)

Task Number and Description	Required or Optional	Page
<i>Task 13: Configure the Switch to the Management Application.</i>	Required if the management server is installed.	2-76
<i>Task 14: Record or Verify Server Restore Information.</i>	Required if the management server is installed.	2-78
<i>Task 15: Verify Switch-to-Server Communication.</i>	Required if the management server is installed.	2-80
<i>Task 16: Configure PFE Key (Optional).</i>	Optional - configure if a product feature enablement (PFE) key is ordered by the customer.	2-82
<i>Task 17: Configure Management Server (Optional).</i>	Optional - configure for open-systems host control of the switch.	2-86
<i>Task 18: Set Switch Date and Time.</i>	Required if the management server is installed.	2-86
<i>Task 19: Configure the Sphereon 4500 Element Manager Application.</i>	Required if the management server is installed.	2-88
<i>Task 20: Back Up Configuration Data.</i>	Required if the management server is installed.	2-115
<i>Task 21: Cable Fibre Channel Ports.</i>	Required.	2-120
<i>Task 22: Configure Zoning (Optional).</i>	Optional - perform this task to configure zoning.	2-121
<i>Task 23: Connect Switch to a Fabric Element (Optional).</i>	Optional - perform this task to connect the switch to a Fibre channel fabric.	2-125
<i>Task 24: Register with the McDATA File Center.</i>	Required.	2-127

Task 1: Verify Installation Requirements

Verify the following requirements are met prior to switch, SANpilot interface, or management server installation. Ensure:

- A site plan is prepared, configuration planning tasks are complete, planning considerations are evaluated, and related planning checklists are complete. Refer to *McDATA Products in a SAN Environment - Planning Manual* (620-000124) for information.
- Storage area network (SAN), director, fabric switch, and Fibre Channel arbitrated loop (FC-AL) device connectivity are evaluated, and the related planning worksheet is complete. Refer to the *McDATA Products in a SAN Environment - Planning Manual* (620-000124) for information.

- Support is available for one of the following switch management methods:
 - A browser-capable PC and Internet connectivity to support switch management through the SANpilot interface, or
 - A browser-capable PC and LAN segment connectivity to the rack-mount management server to support switch management through the SAN management (SANavigator 4.0 or EFCM 8.0) and Element Manager applications.
- Support equipment and technical personnel are available for the installation.
- The required number and type of fiber-optic jumper cables are delivered and available. Ensure the cables are the correct length with the required connectors.
- A customer-supplied 19-inch equipment rack and associated hardware are available (optional).
- Remote workstations or simple network management protocol (SNMP) workstations are available (optional). Workstations are customer-supplied and connected through a corporate or dedicated LAN.

Task 2: Unpack, Inspect, and Install the Ethernet Hub (Optional)

The Sphereon 4500 Switch is managed through either:

- An Internet connection to a browser-capable PC (SANpilot interface). Connection of a LAN segment with multiple switches to the Internet may require installation of the McDATA 24-port Ethernet hub.
- A 10/100 megabit per second (Mbps) LAN connection to both the management server and a browser-capable PC. Connectivity may require installation of the McDATA 24-port Ethernet hub. A combination of up to 48 McDATA products can be configured and managed on one network, therefore multiple, daisy-chained hubs may be required to provide sufficient port connections.

The following paragraphs provide instructions to unpack and inspect one or more Ethernet hubs, and install the hubs in a desktop or rack-mount configuration.

If the customer's existing Ethernet LAN segment is adequate for connectivity and the hub is not delivered, this task is not required. Go to [Task 3: Unpack, Inspect, and Install the Switch](#) on page 2-10.

If the hub is delivered as part of an FC-512 Fabriccenter equipment cabinet, refer to the *McDATA FC-512 Fabriccenter Equipment Cabinet Installation and Service Manual* (620-000100) for instructions, go to [Task 5: Configure Switch Network Information \(Optional\)](#) on page 2-41.

Unpack and Inspect the Ethernet Hub

Unpack and inspect the Ethernet hub(s) as follows:

1. Inspect shipping container(s) for damage caused during transit. If a container is damaged, ensure a representative from the freight carrier is present when the container is opened.
2. Unpack shipping container(s) and inspect each item for damage. Ensure the packaged items correspond to the items listed on the enclosed bill of materials.
3. If any items are damaged or missing, contact the McDATA Solution Center as follows:

Phone: (800) 752-4572 or (720) 566-3910

Fax: (720) 566-3851

E-mail: support@mcddata.com

Desktop Installation

To install and configure up to three Ethernet hubs on a desktop:

1. Remove the backing from the four adhesive rubber pads and apply the pads to the underside of each hub. Ensure the pads are aligned with the scribed circles at each corner.
2. Position the first hub on a table or desktop as directed by the customer.
3. Stack the remaining hubs on top of the first hub as shown in [Figure 2-1](#) on page 2-7. Ensure the adhesive rubber pads on the underside of a hub align with the recesses on the top of the hub below.

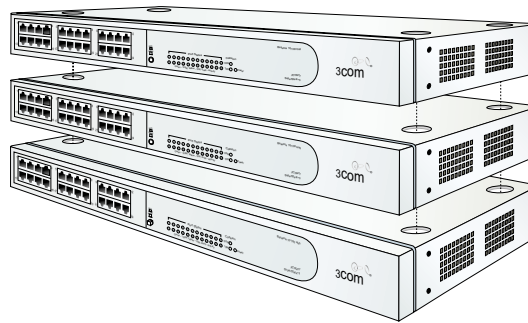


Figure 2-1 Stacked Ethernet Hubs

4. To daisy-chain (connect) the hubs:
 - a. To connect the top and middle hubs in the stack, connect an RJ-45 patch cable to port **24** of the top hub, then connect the cable to port **12** of the middle hub.
 - b. To connect the bottom and middle hubs in the stack, connect a second RJ-45 patch cable to port **24** of the middle hub, then connect the cable to port **12** of the bottom hub.
 - c. Using a pencil or other pointed instrument, set the medium-dependent interface (MDI) switch on the top and middle hubs to **MDI (in)**. Set the MDI switch on the bottom hub to **MDIX (out)**. The configuration is shown in [Figure 2-2](#).

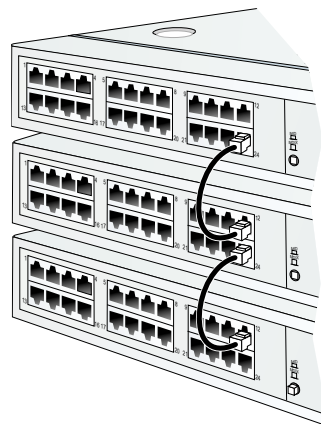


Figure 2-2 Patch Cable and MDI Selector Configuration

NOTE: To connect two hubs, use [step b](#) and [step c](#) (middle and bottom hub instructions only).

5. Connect the U. S. power cord to the receptacle at the rear of each hub and to an AC power strip. Use an 18-inch electrical extension cord if required.
6. Connect the AC power strip to a facility power outlet. Power for each hub switches on when the strip is connected to facility AC power.
7. Inspect the front panel of each hub. Ensure each green **Power** light-emitting diode (LED) illuminates.

Rack-Mount Installation

Perform the following steps to install and configure up to three Ethernet hubs in a Fabriccenter equipment cabinet or a customer-supplied 19-inch equipment rack. A pointed instrument (pencil tip or bent paper clip), #2 Phillips screwdriver, and 1/8-inch Allen wrench are required.

1. Secure one mounting bracket to each side of the first hub as shown in [Figure 2-3](#). Use the two brackets and four pan-head Phillips screws (8/32 x 0.5-inch) provided.

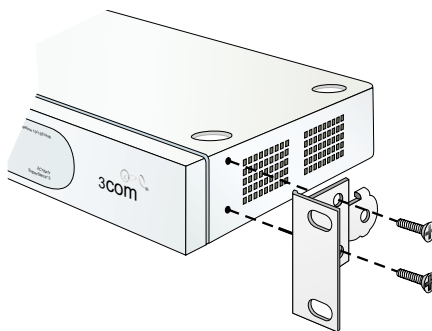


Figure 2-3 Mounting Bracket Installation (Ethernet Hub)

2. Position the first hub in the equipment rack as directed by the customer. Align screw holes in the mounting brackets with screw holes in the rack-mount standards.

NOTE: The hub is 1.75 inches, or one rack unit (1U) high.

3. Secure both sides of the hub to the rack-mount standards as shown in [Figure 2-4](#). Use the 1/8-inch Allen wrench and four Allen-head mounting screws (10/32 x 0.5-inch) provided.

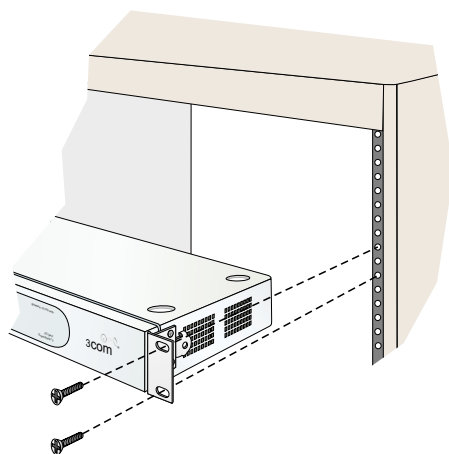


Figure 2-4 Rack Installation (Ethernet Hub)

4. Repeat [step 1](#) through [step 3](#) for the second and third hubs.
5. To daisy-chain (connect) the hubs:
 - a. To connect the top and middle hubs in the stack, connect an RJ-45 patch cable to port **24** of the top hub, then connect the cable to port **12** of the middle hub.
 - b. To connect the bottom and middle hubs in the stack, connect a second RJ-45 patch cable to port **24** of the middle hub, then connect the cable to port **12** of the bottom hub.
 - c. Using a pencil or other pointed instrument, set the medium-dependent interface (MDI) switch on the top and middle hubs to **MDI (in)**. Set the MDI switch on the bottom hub to **MDIX (out)**. The configuration is shown in [Figure 2-2](#) on page 2-7.

NOTE: To connect two hubs, use [step a](#) and [step c](#) (top and middle hub instructions only).

6. Connect an AC power cord to the receptacle at the rear of each hub and to a rack power strip. Power for each hub switches on when the hub (and equipment rack) are connected to facility AC power.

NOTE: Ensure each hub is connected to a separate rack power strip.

7. Inspect the front panel of each hub. Ensure each green **Power** LED illuminates.

Task 3: Unpack, Inspect, and Install the Switch

The following paragraphs provide instructions to unpack and inspect one or more Sphereon 4500 Switches, and install the switches in a desktop or rack-mount configuration.

If the switch is delivered as part of an FC-512 Fabriccenter equipment cabinet, refer to the *McDATA FC-512 Fabriccenter Equipment Cabinet Installation and Service Manual* (620-000100) for instructions, go to [Task 5: Configure Switch Network Information \(Optional\)](#) on page 2-41.

Unpack and Inspect the Switch

Unpack and inspect the switch(es) as follows:

1. Inspect shipping container(s) for damage caused during transit. If a container is damaged, ensure a representative from the freight carrier is present when the container is opened.
2. Unpack shipping container(s) and inspect each item for damage. Ensure the packaged items correspond to the items listed on the enclosed bill of materials.
3. If any items are damaged or missing, contact the McDATA Solution Center as follows:

Phone: (800) 752-4572 or (720) 566-3910

Fax: (720) 566-3851

E-mail: support@mcddata.com

Desktop Installation

To install the switch on a desktop:

1. Remove the backing from the four adhesive rubber pads and apply the pads to the underside of the switch. Ensure the pads are aligned with the scribed circles at each corner.
2. Position the switch on a table or desktop as directed by the customer. Ensure:

- Grounded AC electrical outlets are available.
 - Adequate ventilation is present, and areas with excessive heat, dust, or moisture are avoided.
 - All planning considerations are met. Refer to *McDATA Products in a SAN Environment - Planning Manual* (620-000124) for information.
3. Verify all field-replaceable units (FRUs), including small form factor pluggable (SFP) optical transceivers and combined cooling fan and power supply assemblies are installed as ordered.
 4. Connect both AC power cords to the right (PS0) and left (PS1) receptacles at the rear of the chassis as shown in [Figure 2-5](#).

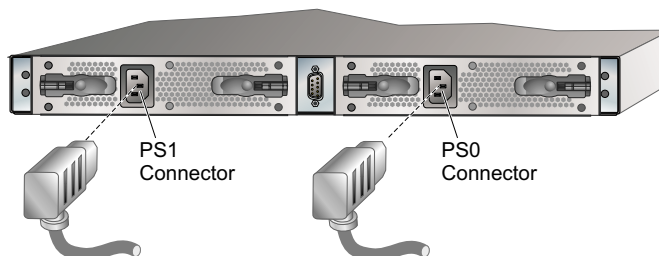


Figure 2-5 AC Power Connections

5. Connect both AC power cords to separate (for redundancy) facility power sources that provide single-phase, 100 to 240 volt alternating current (VAC) current.
6. When the first power cord is connected, the switch powers on and performs power-on self-tests (POSTs). During POSTs:
 - a. The green power (**PWR**) LED on the front panel illuminates.
 - b. The amber system error (**ERR**) LED on the front panel blinks momentarily while the switch is tested.
 - c. The green LED associated with the Ethernet port blinks momentarily while the port is tested.
 - d. The green/blue and amber LEDs associated with Fibre Channel ports blink momentarily while the ports are tested.

7. After successful POST completion, the green power (**PWR**) LED remains illuminated and all other front panel LEDs extinguish.
8. If a POST error or other malfunction occurs, go to [MAP 0000: Start MAP](#) on page 3-6 to isolate the problem.
9. Perform one of the following steps:
 - If the switch is to be managed through the SANpilot interface, go to [Task 4: Configure the Switch at the SANpilot Interface \(Optional\)](#) on page 2-13.
 - If the switch is to be managed through the management server or a customer-supplied server, go to [Task 5: Configure Switch Network Information \(Optional\)](#) on page 2-41.

Rack-Mount Installation

Perform the following steps to install and configure the switch in a Fabriccenter equipment cabinet or a customer-supplied equipment rack. An optional rack-mount kit, T10 Torx tool, and #2 Phillips screwdriver are required.

1. Locate the rack-mount position as directed by the customer. The switch is 1.75 inches, or 1U high.
2. Verify all FRUs, including SFP optical transceivers and combined cooling fan and power supply assemblies are installed as ordered.
3. Open the rack-mount kit and inspect the contents. Refer to the enclosed bill of materials and verify all parts are delivered.
4. Using a T10 Torx tool and #2 Phillips screwdriver, install the switch in the equipment cabinet. Refer to *Sphereon 4500 Switch Rack-Mount Kit Installation Instructions* (958-000267) for guidance.
5. Connect both AC power cords to the right (**PS0**) and left (**PS1**) receptacles at the rear of the chassis as shown in [Figure 2-5](#) on page 2-11.
6. Connect both AC power cords to separate (for redundancy) facility power sources that provide single-phase, 100 to 240 VAC current.
7. When the first power cord is connected, the switch powers on and performs POSTs. During POSTs:

- a. The green power (**PWR**) LED on the front panel illuminates.
 - b. The amber system error (**ERR**) LED on the front panel blinks momentarily while the switch is tested.
 - c. The green LED associated with the Ethernet port blinks momentarily while the port is tested.
 - d. The green/blue and amber LEDs associated with Fibre Channel ports blink momentarily while the ports are tested.
8. After successful POST completion, the green power (**PWR**) LED remains illuminated and all other front panel LEDs extinguish.
 9. If a POST error or other malfunction occurs, go to [MAP 0000: Start MAP](#) on page 3-6 to isolate the problem.
 10. Perform one of the following steps:
 - If the switch is to be managed through the SANpilot interface, go to [Task 4: Configure the Switch at the SANpilot Interface \(Optional\)](#) below.
 - If the switch is to be managed through the management server or a customer-supplied server, go to [Task 5: Configure Switch Network Information \(Optional\)](#) on page 2-41.

Task 4: Configure the Switch at the SANpilot Interface (Optional)

To configure the Sphereon 4500 Switch from the SANpilot interface, selectively perform the following configuration tasks according to the customer's installation requirements:

- Configure switch ports.
- Configure the switch identification, date and time, operating parameters, fabric parameters, and network addresses.
- Configure SNMP trap message recipients, enable the command line interface (CLI), and configure the open systems management server (OSMS) feature.
- Configure administrator and operator passwords.
- Install switch product feature enablement (PFE) keys.

Perform procedures under this task to configure the switch from the SANpilot interface. A PC platform with Internet access and standard web browser running Netscape Navigator 4.6 or higher or Microsoft Internet Explorer 4.0 or higher is required.

1. Connect the switch to the Internet or Ethernet LAN segment as follows:
 - a. Connect one end of the Ethernet patch cable (supplied with the switch) to the RJ-45 connector (labelled **10/100**) on the left front of the switch chassis.
 - b. Connect the remaining end of the Ethernet cable as follows:
 - Connect the cable to an Internet port or Internet-connected LAN segment as directed by the customer's network administrator, or
 - If the McDATA-supplied Ethernet hub installed in [Task 2: Unpack, Inspect, and Install the Ethernet Hub \(Optional\)](#) on page 2-5 provides Internet connectivity, connect the cable to any available hub port.
2. Open the SANpilot interface as follows:
 - a. Ensure the browser-capable PC and the Ethernet LAN segment (with the Sphereon 4500 Switch attached) are connected through the Internet. At the PC, launch the browser application (Netscape Navigator or Internet Explorer).
 - b. At the browser, enter the Internet Protocol (IP) address of the switch as the Internet uniform resource locator (URL). Use the default IP address of **10.1.1.10**. The *Enter Network Password* dialog box displays ([Figure 2-6](#)).



Figure 2-6 Enter Network Password Dialog Box

- c. Type the default user name and password.

NOTE: The default SANpilot interface user name is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

- d. Click OK. The SANpilot interface opens with the *View* panel open and the *Director* page displayed (Figure 2-7).

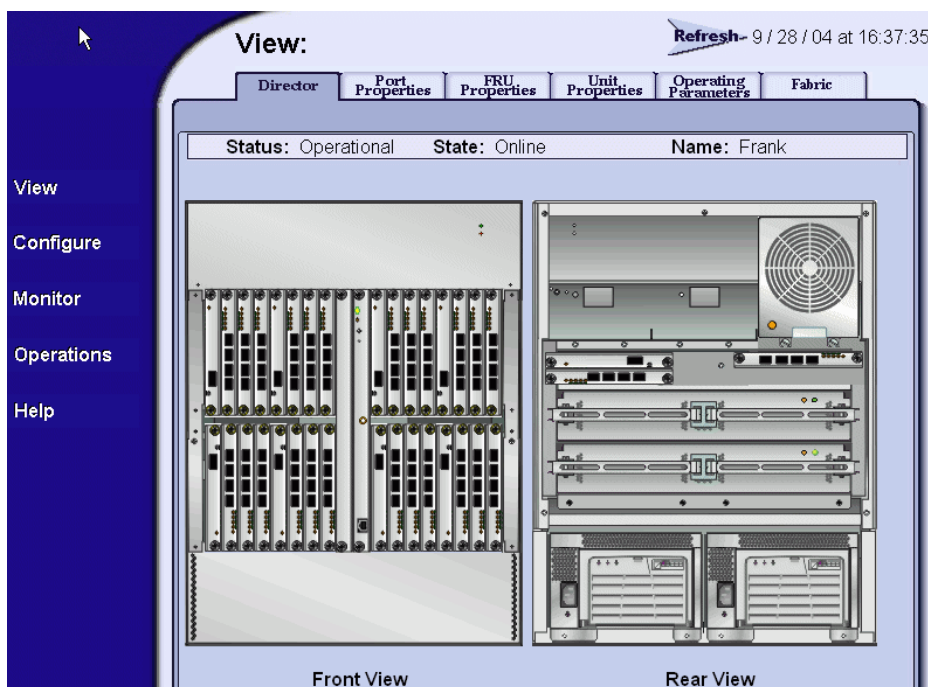


Figure 2-7 View Panel (Director Page)

Configure Switch Ports

Perform procedures in this section to configure names and operating characteristics for Fibre Channel ports. To configure one or more switch ports:

1. At the *View* panel, select the *Configure* option at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed (Figure 2-8 on page 2-16).

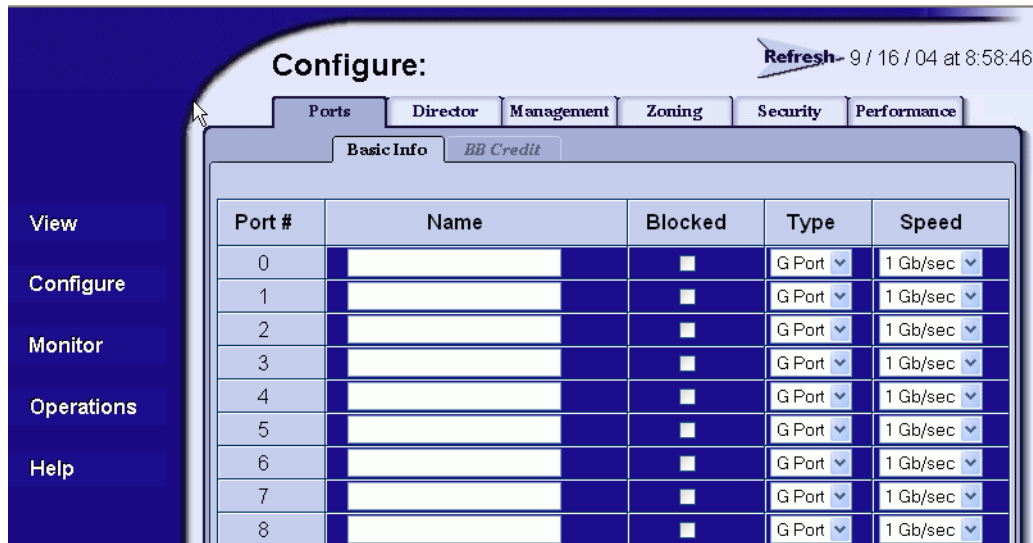


Figure 2-8 Configure Panel (Ports Page)

- For each port to be configured, type a port name of 24 alphanumeric characters or less in the associated *Name* field. The port name should characterize the device to which the port is attached.
- Click a check box in the *Blocked* column to block or unblock a port (default is unblocked). A check mark in the box indicates a port is blocked. Blocking a port prevents the attached device or fabric switch from communicating. A blocked port continuously transmits the offline sequence (OLS).
- Click the check box in the *FAN* column to enable or disable the fabric address notification (FAN) feature (default is enabled). A check mark in the box indicates FAN is enabled. When the feature is enabled, the port transmits FAN frames after loop initialization to verify that FC-AL devices are still logged in. It is recommended this option be enabled for ports configured for loop operation.
- Select from the drop-down list in the *Type* column to configure the port type. Available selections are:
 - Fabric port (**F_Port**).
 - Expansion port (**E_Port**).

- Generic port (**G_Port**). A generic port setting allows F_Port and E_Port behavior only.
 - Generic mixed port (**GX_Port**). A generic mixed port setting allows F_Port, fabric loop port (FL_Port), and E_Port behavior. This is the default selection.
 - Fabric mixed port (**FX_Port**). A fabric mixed port setting allows F_Port and FL_Port behavior only.
- e. Select from the drop-down list in the *Speed* column to configure the port transmission rate. Available selections are:
- Auto-negotiate between 1.0625 and 2.125 gigabit per second (Gbps) operation (**Negotiate**). This is the default selection.
 - 1.0625 Gbps operation (**1 Gb/sec**).
 - 2.125 Gbps operation (**2 Gb/sec**).
2. Click *Activate* to save and activate the changes. The message **Your changes to the port configuration have been successfully activated** appears.

Configure Switch Identification

Perform this procedure to configure the switch name, description, location, and contact person. The *Name*, *Location*, and *Contact* variables configured here correspond respectively to the SNMP variables *sysName*, *sysLocation*, and *sysContact*. These variables are used by SNMP management workstations when obtaining data from managed switches. To configure the switch identification:

1. At the *Configure* panel, click the *Switch* tab. The *Switch* page displays with the *Identification* tab selected (Figure 2-9 on page 2-18).
 - a. Type a switch name of 24 alphanumeric characters or less in the *Name* field. Each switch should be configured with a unique name.

If the switch is installed on a public LAN, the name should reflect the switch's Ethernet network domain name system (DNS) host name. For example, if the DNS host name is **sphereon4500.mcdata.com**, the name entered in this dialog box should be **sphereon4500**.

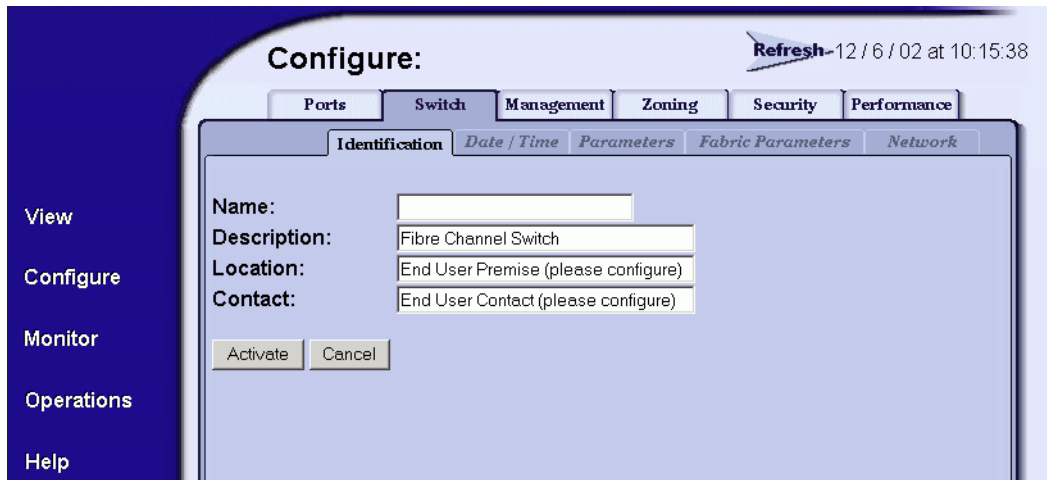


Figure 2-9 Configure Panel (Switch Page with Identification Tab)

- b. Type a switch description of 255 alphanumeric characters or less in the *Description* field.
 - c. Type the switch's physical location (255 alphanumeric characters or less) in the *Location* field.
 - d. Type the name of a contact person (255 alphanumeric characters or less) in the *Contact* field.
2. Click *Activate* to save and activate the changes. The message **Your changes to the identification configuration have been successfully activated** appears.

Configure Date and Time

Perform this procedure to configure the effective date and time for the switch. To set the date and time:

1. At the *Configure* panel, click the *Date/Time* tab. The *Switch* page displays with the *Date/Time* tab selected (Figure 2-10 on page 2-19).

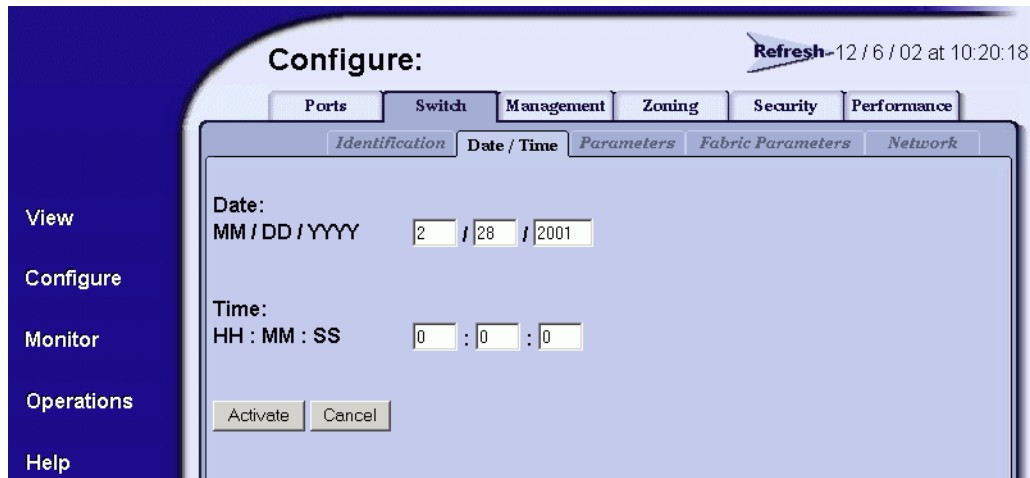


Figure 2-10 Configure Panel (Switch Page with Date/Time Tab)

- a. Click the *Date* fields that require change, and type numbers in the following ranges:
 - Month (MM): 1 through 12.
 - Day (DD): 1 through 31.
 - Year (YYYY): greater than 1980.
- b. Click the *Time* fields that require change, and type numbers in the following ranges:
 - Hour (HH): 0 through 23.
 - Minute (MM): 0 through 59.
 - Second (SS): 0 through 59.
2. Click *Activate* to save and activate the changes. The message **Your changes to the date/time configuration have been successfully activated** appears.

Configure Operating Parameters

Perform this procedure to configure the switch's preferred domain ID, insistent domain ID, rerouting delay, and domain registered state change notifications (RSCNs). The switch must be set offline to configure the preferred domain ID. To configure parameters:

1. Set the switch offline as follows:
 - a. At the *Configure* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens and the *Switch* page displays with the *Beacon* tab selected
 - b. Click the *Online State* tab, then click *Set Offline*. The message **Your operations changes have been successfully activated** appears.
2. At the *Operations* panel, select the *Configure* option at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed.
3. At the *Configure* panel, click the *Switch* tab, then click the *Parameters* tab. The *Switch* page displays with the *Parameters* tab selected (Figure 2-11).

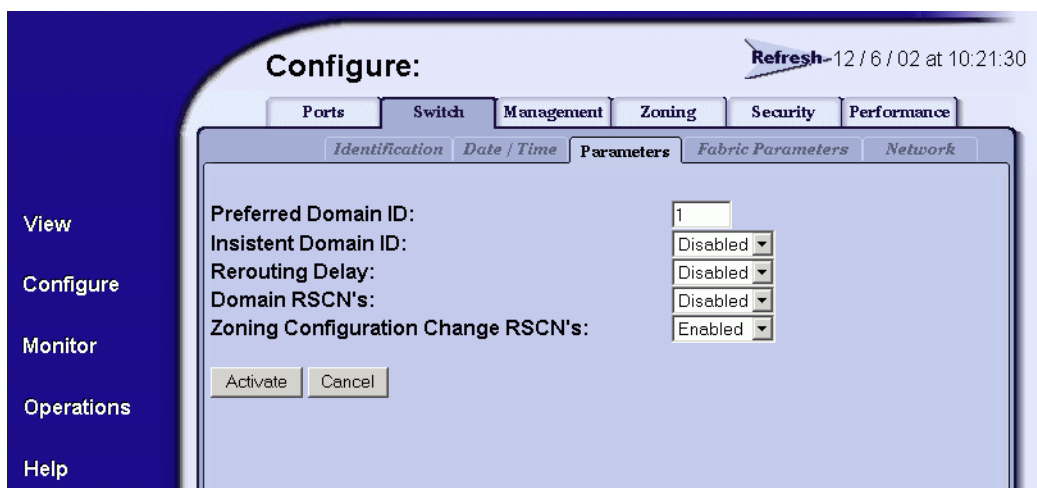


Figure 2-11 Configure Panel (Switch Page with Parameters Tab)

- a. At the *Preferred Domain ID* field, type a value between 1 through 31. The domain ID uniquely identifies each switch in a fabric.

NOTE: If the switch is attached to a fabric element, the switch and element must have unique domain IDs. If the values are not unique, the E_Port connection to the element segments and the switch cannot communicate with the fabric.

- b. At the *Insistent Domain ID* field, select *Enabled* or *Disabled*. When this parameter is enabled, the domain ID configured in the *Preferred Domain ID* field becomes the active domain identification when the fabric initializes.
 - c. At the *Rerouting Delay* field, select *Enabled* or *Disabled*. When this parameter is enabled, traffic is delayed through the fabric by the specified error detect time out value (E_D_TOV). This delay ensures Fibre Channel frames are delivered to their destination in order, even if a change to the fabric topology creates a new (shorter) transmission path.
 - d. At the *Domain RSCNs* field, select *Enabled* or *Disabled*. When this parameter is enabled, attached devices can register to receive notification when another attached device changes state.
4. Click *Activate* to save and activate the changes. The message **Your changes to the operating parameters configuration have been successfully activated** appears.
5. If fabric parameters require configuration, go to [Configure Fabric Parameters](#) below. If the configuration is complete, set the switch online as follows:
 - a. At the *Configure* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens and the *Switch* page displays with the *Beacon* tab selected
 - b. Click the *Online State* tab, then click *Set Online*. The message **Your operations changes have been successfully activated** appears.

Configure Fabric Parameters

Perform this procedure to configure the fabric operating parameters, including resource allocation time out value (R_A_TOV), E_D_TOV, switch priority, and interop mode. The switch must be set offline. To configure parameters:

1. If required, set the switch offline as follows:
 - a. At the *Configure* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens and the *Switch* page displays with the *Beacon* tab selected
 - b. Click the *Online State* tab, then click *Set Offline*. The message **Your operations changes have been successfully activated** appears.

2. At the *Operations* panel, select the *Configure* option at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed.
3. At the *Configure* panel, click the *Switch* tab, then click the *Fabric Parameters* tab. The *Switch* page displays with the *Fabric Parameters* tab selected (Figure 2-12).

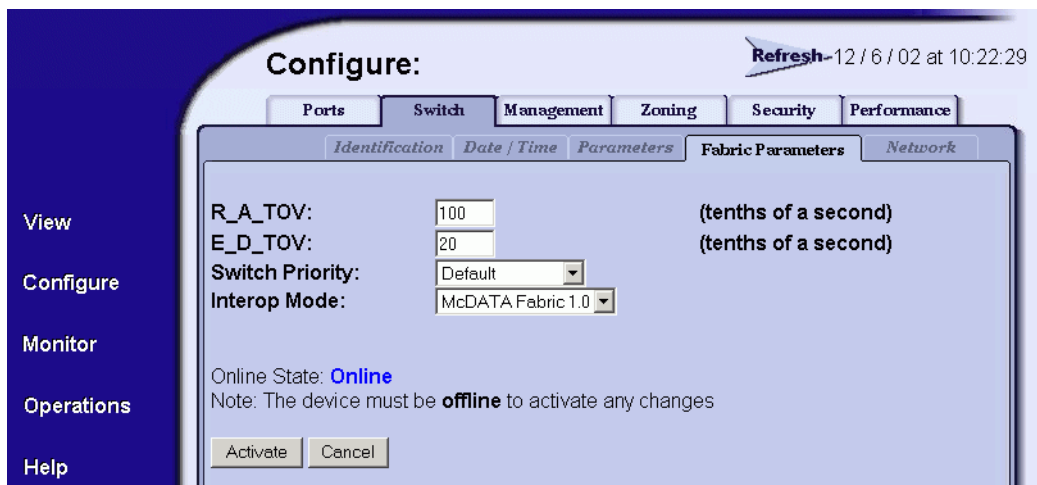


Figure 2-12 Configure Panel (Switch Page with Fabric Parameters Tab)

- a. At the *R_A_TOV* field, type a value between **10** through **1200** tenths of a second (one through 120 seconds). Ten seconds (**100**) is the recommended value.

NOTE: If the switch is attached to a fabric element, the switch and element must be set to the same *R_A_TOV* value. If the values are not identical, the *E_Port* connection to the element segments and the switch cannot communicate with the fabric. In addition, the *R_A_TOV* value must be greater than the *E_D_TOV* value.

- b. At the *E_D_TOV* field, type a value between **2** through **600** tenths of a second (0.2 through 60 seconds). Two seconds (**20**) is the recommended value.

NOTE: If the switch is attached to a fabric element, the switch and element must be set to the same E_D_TOV value. If the values are not identical, the E_Port connection to the element segments and the switch cannot communicate with the fabric. In addition, the E_D_TOV value must be less than the R_A_TOV value.

- c. Select from the *Switch Priority* drop-down list to set the switch priority. Available selections are *Default*, *Principal*, and *Never Principal*. The default setting is *Default*.

This value designates the fabric's principal switch. The principal switch is assigned a priority of **1** and controls the allocation and distribution of domain IDs for all fabric elements (including itself).

Principal is the highest priority setting, *Default* is the next highest, and *Never Principal* is the lowest priority setting. The setting *Never Principal* means the switch is incapable of becoming a principal switch. If all switches are set to *Principal* or *Default*, the switch with the highest priority and the lowest world wide name (WWN) becomes the principal switch.

At least one switch in a fabric must be set as *Principal* or *Default*. If all switches are set to *Never Principal*, all interswitch links (ISLs) segment.

- d. Select from the *Interop Mode* drop-down list to set the switch operating mode. This setting only affects the mode used to manage the switch; it does not affect port operation. Available selections are:
- **McDATA Fabric 1.0** - Select this option if the switch is fabric-attached only to other McDATA directors or switches operating in McDATA fabric mode.
 - **Open Fabric 1.0** - Select this option (default) for managing heterogeneous fabrics and if the switch is fabric-attached to McDATA directors or switches and open-fabric compliant switches produced by other original equipment manufacturers (OEMs).

NOTE: When Open Fabric 1.0 is selected, the default zone is disabled, and you have to activate the default zone or enable the active zone set

4. Click *Activate* to save and activate the changes. The message **Your changes to the fabric parameters configuration have been successfully activated** appears.
5. Set the switch online as follows:
 - a. At the *Configure* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens and the *Switch* page displays with the *Beacon* tab selected
 - b. Click the *Online State* tab, then click *Set Online*. The message **Your operations changes have been successfully activated** appears.

Configure Network Information

Verify the type of LAN installation with the customer's network administrator. If one switch is installed on a dedicated LAN, network information (IP address, subnet mask, and gateway address) does not require change. Go to [Configure SNMP](#) on page 2-26.

If multiple switches are installed or a public LAN segment is used, network information must be changed to conform to the customer's LAN addressing scheme.

Perform the following steps to change a switch's IP address, subnet mask, or gateway address.

1. At the *Operations* panel, select the *Configure* option at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed.
2. At the *Configure* panel, click the *Switch* tab, then click the *Network* tab. The *Switch* page displays with the *Network* tab selected ([Figure 2-13](#)).

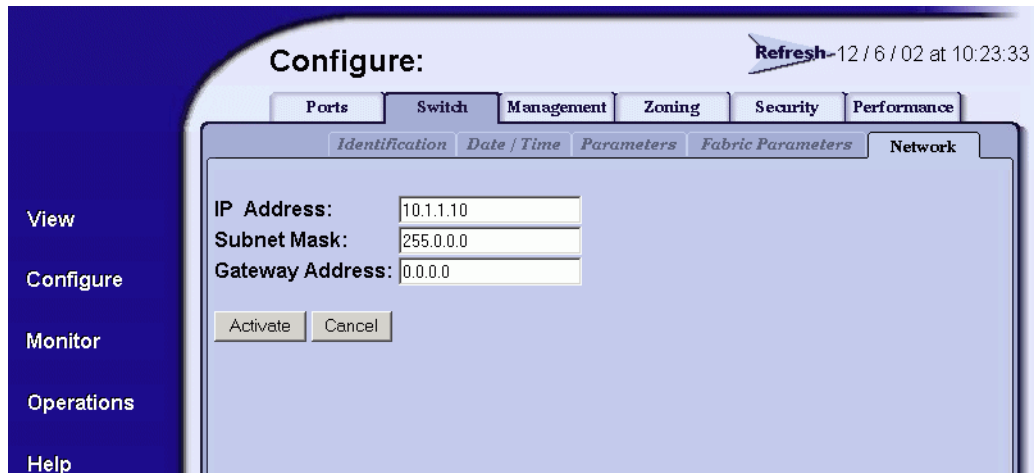


Figure 2-13 Configure Panel (Switch Page with Network Tab)

- a. At the *IP Address* field, type the new value as specified by the customer's network administrator (default is **10.1.1.10**).
 - b. At the *Subnet Mask* field, type the new value as specified by the customer's network administrator (default is **255.0.0.0**).
 - c. At the *Gateway Address* field, type the new value as specified by the customer's network administrator (default is **0.0.0.0**).
3. Click *Activate* to save and activate the changes. The following message box displays (Figure 2-14).

Your changes to the Network configuration have been successfully activated. The following Network information has been configured to the switch:

IP Address:	10.1.1.10
Gateway Address:	0.0.0.0
Subnet Mask:	255.0.0.0

In order to re-establish your browser management connection, you must update local ARP tables on your operating system and direct your web browser to the new IP Address displayed above. Please consult the Installation and Service Manual provided with this product for more information.

Figure 2-14 Network Information Message Box

4. Update the address resolution protocol (ARP) table for the browser PC.
 - a. Select the *Exit* option from the *File* menu to close the SANpilot interface and browser applications. The Windows desktop displays.
 - b. At the Windows desktop, click *Start* at the left side of the task bar. The *Windows Workstation* menu displays.
 - c. At the *Windows Workstation* menu, sequentially select the *Programs* and *Command Prompt* options. A disk operating system (DOS) window displays.
 - d. Delete the switch's *old* IP address from the ARP table. At the command (C:\) prompt, type **arp -d xxx.xxx.xxx.xxx**, where **xxx.xxx.xxx.xxx** is the old IP address for the switch.
 - e. Click close (X) at the upper right corner of the DOS window to close the window and return to the Windows desktop.
5. At the switch front panel, press and hold the **IML/RESET** button for ten seconds. The switch performs a power-on reset (POR).
6. At the PC, launch the browser application (Netscape Navigator or Internet Explorer).
7. At the browser, enter the switch's *new* IP address as the Internet URL. The *Enter Network Password* dialog box displays.
8. Type the default user name and password.

NOTE: The default user name is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

9. Click OK. The SANpilot interface opens with the *View* panel open and the *Switch* page displayed.

Configure SNMP

Perform this procedure to configure community names, write authorizations, network addresses, and user datagram protocol (UDP) port numbers for up to six SNMP trap message recipients. A trap recipient is a management workstation that receives notification (through SNMP) if a switch event occurs. To configure SNMP trap recipients:

1. At the *View* panel, select the *Configure* option at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed.

2. At the *Configure* panel, click the *Management* tab. The *Management* page displays with the *SNMP* tab selected (Figure 2-15 on page 2-27).
 - a. Click the *Enable SNMP Agent* check box to enable or disable the installed SNMP agent.
 - b. Select the appropriate Fibre Alliance management information base (FA MIB) from the *FA MIB Version* drop-down list. Available selections are:
 - **FA MIB Version 3.0.**
 - **FA MIB Version 3.1.**
 - c. Click the *Enable Authentication Traps* check box to enable or disable transmission of SNMP trap messages to configured recipients.

The screenshot shows the 'Configure' panel with the 'Management' tab selected. The 'SNMP' sub-tab is active. The interface includes a sidebar with 'View', 'Configure', 'Monitor', 'Operations', and 'Help'. The main area has a 'Refresh' button and a timestamp '5 / 28 / 03 at 10:35:19'. Below the tabs, there are checkboxes for 'Enable SNMP Agent' (checked) and 'Enable Authentication Traps' (unchecked). A dropdown menu for 'FA MIB Version' is set to 'FA MIB 3.1'. A table with four columns: 'Community Name', 'Write Authorization', 'Trap Recipient', and 'UDP Port Number' is displayed. The first row has 'public' in the 'Community Name' field and checkboxes in the 'Write Authorization' column. At the bottom are 'Activate' and 'Cancel' buttons.

Community Name	Write Authorization	Trap Recipient	UDP Port Number
public	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		

Figure 2-15 Configure Panel (Management Page with SNMP Tab)

- d. For each trap recipient to be configured, type a community name of 32 alphanumeric characters or less in the *Community Name* field. The community name is incorporated in SNMP trap messages to ensure against unauthorized viewing or use.

- e. Click the check box in the *Write Authorization* column to enable or disable write authorization for the trap recipient (default is disabled). A check mark indicates write authorization is enabled. When the feature is enabled, a management workstation user can change *sysContact*, *sysName*, and *sysLocation* SNMP variables.
 - f. Type the IP address or DNS host name of the trap recipient (SNMP management workstation) in the *Trap Recipient* field. It is recommended the IP address be used.
 - g. The default UDP port number for trap recipients is **162**. Type a decimal port number in the *UDP Port Number* field to override the default value.
3. Click *Activate* to save and activate the changes. The message **Your changes to the SNMP configuration have been successfully activated** appears.

Enable or Disable the CLI

Perform this procedure to toggle (enable or disable) the state of the switch's command line interface. To change the CLI state:

1. At the *Configure* panel, click the *CLI* tab. The *Management* page displays with the *CLI* tab selected (Figure 2-16).

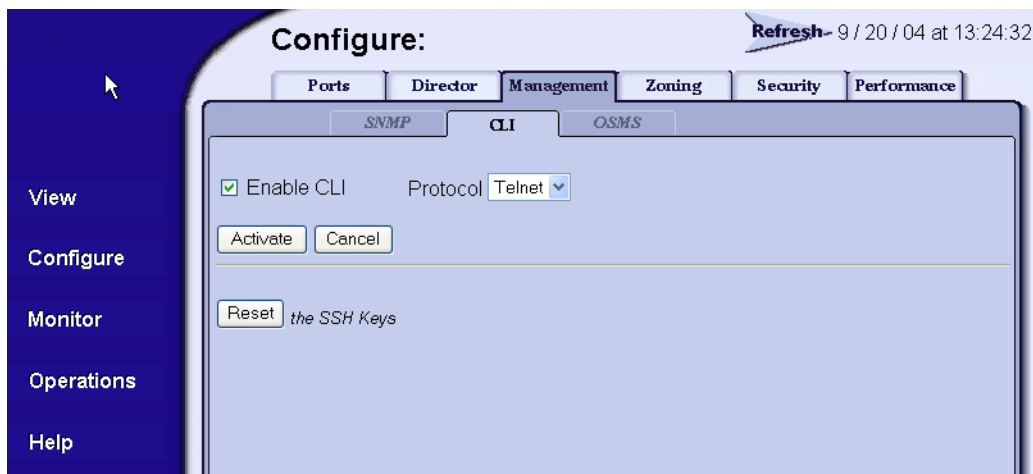


Figure 2-16 Configure Panel (Management Page with CLI Tab)

2. Perform one of the following steps as required:

- Click *Enable* to activate the CLI. The message **Your changes to the CLI enable state have been successfully activated** appears.
- Click *Disable* to deactivate the CLI. The message **Your changes to the CLI enable state have been successfully activated** appears.

Enable or Disable Host Control

Perform this procedure to toggle (enable or disable) host control of the switch through the OSMS. The OSMS feature must be installed to access this control. Refer to [Install PFE Keys \(Optional\)](#) on page 2-38 for instructions. If the feature is not installed, the message **OSMS Feature Not Installed** appears. To enable or disable host control:

1. At the *Configure* panel, click the *OSMS* tab. The *Management* page displays with the *OSMS* tab selected ([Figure 2-17](#)).

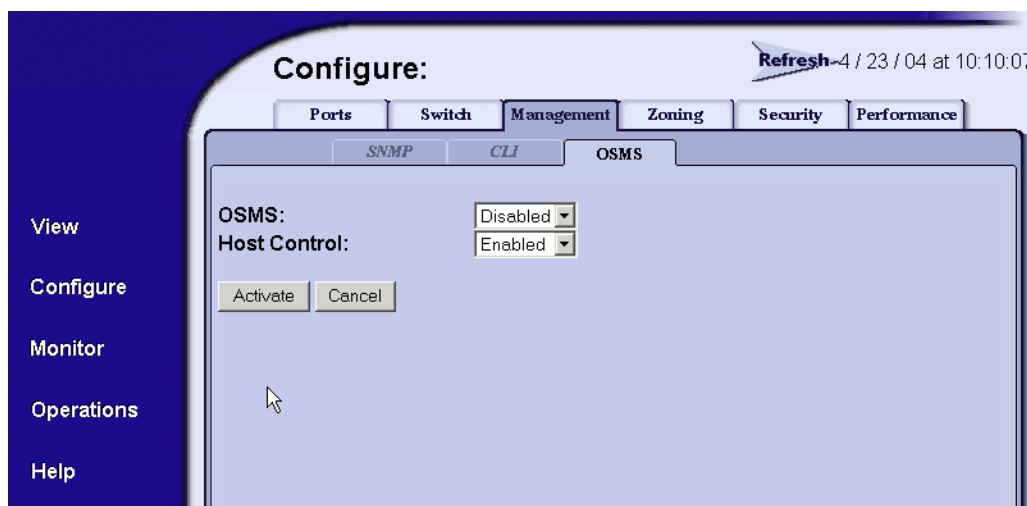


Figure 2-17 Configure Panel (Management Page with OSMS Tab)

2. Perform one of the following steps as required:
 - Click *Enable* to activate the OSMS. The message **Your changes to the host control enable state have been successfully activated** appears.
 - Click *Disable* to deactivate the OSMS. The message **Your changes to the host control enable state have been successfully activated** appears.

Configure User Rights

Perform this procedure to configure the administrator-level and operator-level passwords used to access the SANpilot interface through the *Enter Network Password* dialog box. To configure passwords:

1. At the *Configure* panel, click the *Security* tab. The *Security* page displays with the *User Rights* tab selected (Figure 2-18 on page 2-30).

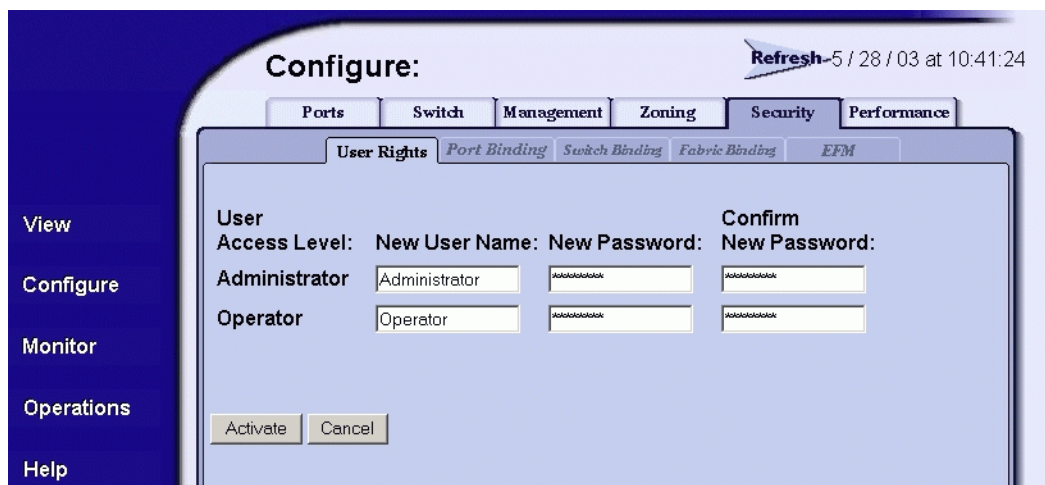


Figure 2-18 Configure Panel (Security Page with User Rights Tab)

2. For the *Administrator* set of data fields:
 - a. Type the administrator user name (as specified by the customer's network administrator) in the *New User Name* field. Use 16 alphanumeric characters or less.
 - b. Type the administrator password (as specified by the customer's network administrator) in the *New Password* field. Use 16 alphanumeric characters or less.
 - c. Type the administrator password again in the *Confirm New Password* field.
3. For the *Operator* set of data fields:
 - a. Type the operator user name (as specified by the customer's network administrator) in the *New User Name* field. Use 16 alphanumeric characters or less.

- b. Type the operator password (as specified by the customer's network administrator) in the *New Password* field. Use 16 alphanumeric characters or less.
 - c. Type the operator password again in the *Confirm New Password* field.
4. Click *Activate* to save the information. The message **Your changes to the user rights configuration have been successfully activated** appears.

Configure Port Binding

Perform this procedure to configure Fibre Channel port binding by WWN. To configure port binding:

1. At the *Configure* panel, click the *Port Binding* tab. The *Security* page displays with the *Port Binding* tab selected (Figure 2-19).

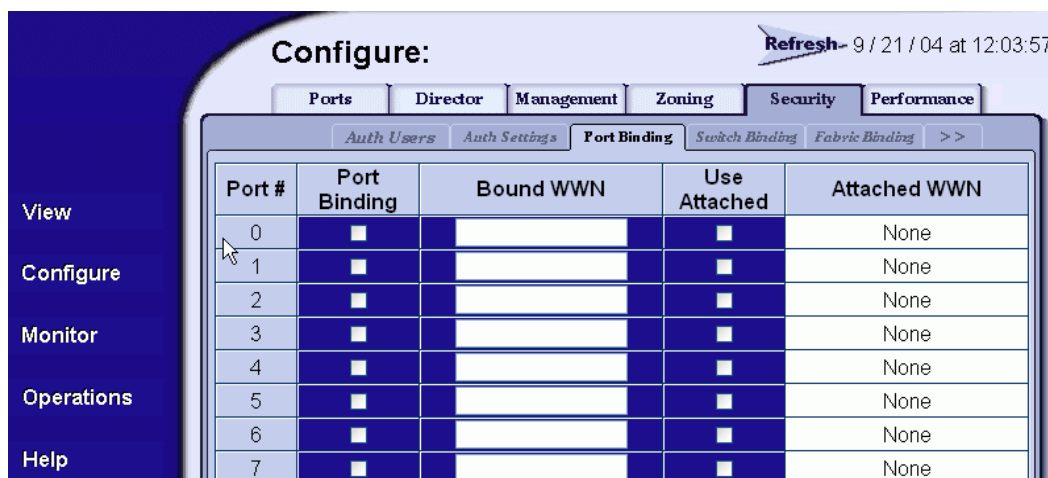


Figure 2-19 Configure Panel (Security Page with Port Binding Tab)

- a. Click the check box in the *Port Binding* column to enable or disable port binding for a specified port (default is disabled).
 - b. In the *Bound WWN* column, type the world wide name of the device to which the port is to be bound. If port binding is enabled, only the specified device can connect to the port. If port binding is enabled and no device is specified in the *Bound WWN* column, then no devices can connect to the port.

- c. The *Attached WWN* column contains read-only fields that list the world wide names of attached Fibre Channel devices. Click the check box in the *Use Attached* column to indicate the world wide name specified in the *Attached WWN* column is to be used for port binding. After activation, the attached WWN appears in the *Bound WWN* column.
2. Click *Activate* to save the information. The message **Your changes to the port binding configuration have been successfully activated** appears.

Configure Switch Binding

Perform this procedure to configure switch binding by attached devices (nodes). The SANtegrity™ feature must be installed to access this control. Refer to [Install PFE Keys \(Optional\)](#) on page 2-38 for instructions. If the feature is not installed, the message **This Feature Not Installed** appears. To configure switch binding:

1. At the *Configure* panel, click the *Switch Binding* tab. The *Security* page displays with the *Switch Binding* tab selected (Figure 2-20).



Figure 2-20 Configure Panel (Security Page with Switch Binding Tab)

2. Select the connection policy from the *Switch Binding State* drop-down list. The switch binding state indicates the type of binding restrictions imposed on the switch. Switch binding is enabled by activating Enterprise Fabric Mode (refer to [Enable or Disable Enterprise Fabric Mode](#) on page 2-35), or by enforcing a connection policy at the *Switch Binding State* drop-down list. Available selections are:
 - **Enable & Restrict E_Ports** - Uses the switch binding membership list to restrict devices that can attach to the switch through E_Ports.
 - **Enable & Restrict F_Ports** - Uses the switch binding membership list to restrict devices that can attach to the switch through F_Ports.
 - **Enable & Restrict All Ports** - Uses the switch binding membership list to restrict devices that can attach to the switch through any port.
 - **Disable Switch Binding** - Sets the switch binding state to disabled and removes restrictions on devices that can attach to the switch.
3. Click *Submit*. A confirmation dialog box appears. Click OK to close the confirmation dialog box, activate the selected connection policy, and change the switch binding state.

NOTE: The **Disable Switch Binding** selection cannot be activated while Enterprise Fabric Mode is enabled and the switch is online.

4. The *Attached Nodes* drop-down list contains the world wide names of attached Fibre Channel devices. To add a member (node or device) to the switch binding membership list displayed at the bottom of the page, perform one of the following:
 - Select a WWN from the *Attached Nodes* drop-down list and click the adjacent *Add Member* button.
 - Type a new WWN in the *Detached Node (WWN)* field and click the adjacent *Add Member* button.
5. To delete a device from the switch binding membership list, click the *Delete* button adjacent to the device WWN. A confirmation dialog box appears. Click OK to close the dialog box and delete the device.

Configure Fabric Binding

Perform this procedure to configure fabric binding by attached fabric member (domain ID and WWN). The SANtegrity feature must be installed to access this control. Refer to [Install PFE Keys \(Optional\)](#) on page 2-38 for instructions. If the feature is not installed, the message **This Feature Not Installed** appears. To configure fabric binding:

1. At the *Configure* panel, click the *Fabric Binding* tab. The *Security* page displays with the *Fabric Binding* tab selected (Figure 2-21).



Figure 2-21 Configure Panel (Security Page with Fabric Binding Tab)

2. The saved status of the fabric binding configuration displays at the top of the page. The status can be:
 - **Saved & Active** - Information displayed on the page reflects the active configuration saved for the fabric.
 - **Unsaved & Active** - Information displayed may be different than the active configuration saved for the fabric.

- **Unsaved & Inactive** - Information displayed may be different than the active configuration saved for the fabric.
3. Click *Save and Activate* to save and activate the displayed fabric binding configuration. A confirmation dialog box appears. Click *OK* to close the confirmation dialog box, activate the fabric binding configuration, and change the status to **Saved & Active**.
 4. Click *Deactivate* to deactivate fabric binding while Enterprise Fabric Mode is also deactivated. A confirmation dialog box appears. Click *OK* to close the confirmation dialog box, deactivate fabric binding, and change the status to **Unsaved & Inactive**.

NOTE: The **Deactivate** selection cannot be used while Enterprise Fabric Mode is enabled.

5. Click *Discard Unsaved Changes* to discard unsaved changes to the fabric binding configuration. A confirmation dialog box appears. Click *OK* to close the confirmation dialog box; then refresh and display the current fabric binding configuration.
6. To add a member (new fabric) to the fabric binding membership list displayed at the bottom of the page, type a new domain ID (range is **1** through **31**) in the *Domain ID* field, type a new WWN in the *WWN* field, and click the adjacent *Add Member* button.
7. To delete a fabric from the fabric binding membership list, click the *Delete* button adjacent to the fabric domain ID and WWN. A confirmation dialog box appears. Click *OK* to close the dialog box and delete the fabric.

Enable or Disable Enterprise Fabric Mode

Perform this procedure to toggle (enable or disable) the use of Enterprise Fabric Mode (EFM). The SANtegrity feature must be installed to access this control. Refer to [Install PFE Keys \(Optional\)](#) on page 2-38 for instructions. If the feature is not installed, the message **This Feature Not Installed** appears. To enable or disable EFM:

1. At the *Configure* panel, click the *EFM* tab. The *Security* page displays with the *EFM* tab selected ([Figure 2-22](#) on page 2-36).

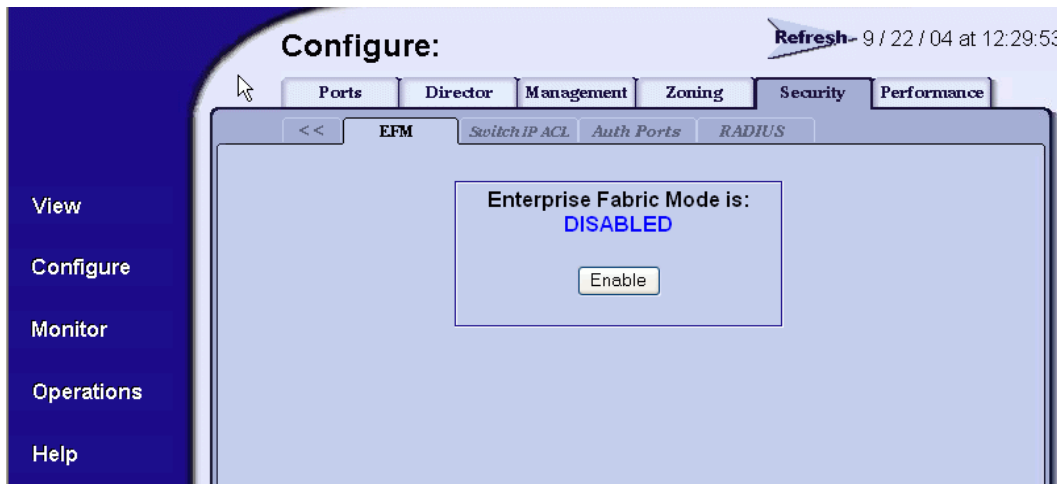


Figure 2-22 Configure Panel (Security Page with EFM Tab)

2. Perform one of the following steps as required:
 - Click *Enable* to activate EFM. The message **Your changes to enterprise fabric mode have been successfully activated** appears.
 - Click *Disable* to deactivate EFM. The message **Your changes to enterprise fabric mode have been successfully activated** appears.

Configure OpenTrunking

Perform this procedure to configure OpenTrunking parameters. The OpenTrunking feature must be installed to access this control. Refer to [Install PFE Keys \(Optional\)](#) on page 2-38 for instructions. If the feature is not installed, the message **OpenTrunking Feature Not Installed** appears. To configure OpenTrunking parameters:

1. At the *Configure* panel, click the *Performance* tab. The *Performance* page displays with the *OpenTrunking* tab selected ([Figure 2-23](#) on page 2-37).

Configure: Refresh 9 / 22 / 04 at 12:32:52

Ports Director Management Zoning Security **Performance**

Open Trunking Preferred Path

Open Trunking State: Enabled ▾
 Unresolved Congestion Event Notification: Disabled ▾
 Backpressure Event Notification: Disabled ▾
 Low BB Credit Threshold: ☐ Default 50 % (1-99%)

0-31		32-63		64-95		96-127		132-143	
Port #	Port Type	Use Default Threshold %		Threshold % (1-99%)					
0	G Port	<input checked="" type="checkbox"/>		66					
1	G Port	<input checked="" type="checkbox"/>		66					
2	G Port	<input checked="" type="checkbox"/>		66					
3	G Port	<input checked="" type="checkbox"/>		66					
4	G Port	<input checked="" type="checkbox"/>		66					

Figure 2-23 Configure Panel (Performance Page with OpenTrunking Tab)

- At the *OpenTrunking State* field, select *Enabled* or *Disabled*. When this parameter is enabled, the optional OpenTrunking feature is functional.
- At the *Unresolved Congestion Event Notification* field, select *Enabled* or *Disabled*. When this parameter is enabled, unresolved congestion events are recorded in the event log, and SNMP trap messages are generated and transmitted (if SNMP is configured).

An unresolved congestion event occurs for a low-BB_Credit ISL when the switch's firmware rerouting algorithm cannot route data flow to an alternate path (because doing so would exceed the alternate path's low BB_Credit threshold).

- At the *Backpressure Event Notification* field, select *Enabled* or *Disabled*. When this parameter is enabled, backpressure events are recorded in the event log, and SNMP trap messages are generated and transmitted (if SNMP is configured).

A backpressure event occurs when the percent time an ISL has low BB_Credit exceeds the low BB_Credit threshold.

d. The low BB_Credit threshold is the percent time an ISL is allowed to not transmit data because BB_Credit is unavailable. When the threshold is exceeded, data is rerouted to another ISL. In addition, traffic cannot be rerouted to another low-threshold ISL. Use one of the following to set the low BB_Credit threshold:

- Click the *Default* check box. A check mark appears in the box and a calculated default value appears (1% to 99%) in the *Low BB_Credit Threshold* field. If the default value is enabled, a value cannot be entered in the *Low BB_Credit Threshold* field.
- Ensure the *Default* check box is blank. At the *Low BB_Credit Threshold* field, type a percentage value from 1% to 99%.

NOTE: The default low BB_Credit threshold is calculated by the switch's firmware and performs well in most cases.

2. For each switch port:

- a. Click the check box in the *Default Threshold %* column. A check mark appears in the box and a calculated default value appears (1% to 99%) in the associated field in the *Threshold %* column. If the default value is enabled, a value cannot be entered in the *Threshold %* column.
- b. Ensure the check box in the *Default Threshold %* column is blank. At the associated field in the *Threshold %* column, type a percentage value from 1% to 99%.

NOTE: The default low BB_Credit threshold is calculated by the switch's firmware and performs well in most cases.

3. Click *Activate* to save the information. The message **Your changes to the port binding configuration have been successfully activated** appears.
4. If additional optional features are to be installed, go to [Install PFE Keys \(Optional\)](#) on page 2-38. If no PFE keys are to be installed, go to [Task 21: Cable Fibre Channel Ports](#) on page 2-120.

Install PFE Keys (Optional)

Perform this procedure to install one or more of the following optional features:

- **OSMS** - These feature allows open systems host control of the switch.
- **Flexport Technology** - A Flexport Technology switch is delivered at a discount with only eight ports enabled. When additional port capacity is required, the remaining ports are enabled (in eight-port increments) through purchase of this feature.
- **SANtegrity™ binding** - This feature enhances security in SANs with a large and mixed group of fabrics and attached devices.
- **OpenTrunking** - This feature provides dynamic load balancing of Fibre Channel traffic across multiple ISLs.
- **Full volatility** - This feature ensures that no Fibre Channel frames are stored after the switch is powered off, and a memory dump file (that possibly includes classified frames) is not included as part of the data collection procedure.
- **CNT WAN support** - This feature is included *only* in software maintenance release 4.02.00, and is required to allow the switch to communicate with Computer Network Technologies (CNT) UltraEdge wide area network (WAN) Gateways.

After purchasing a feature, obtain the required PFE key by following the enclosed instructions. A PFE key is an alphanumeric string consisting of both uppercase and lowercase characters. The total number of characters may vary. The key is case sensitive and must be entered exactly, including dashes. The following is an example of a PFE key format:

XxXx-XXxX-xxXX-xX.

After obtaining the PFE key, install the feature as follows:

1. Set the switch offline as follows:
 - a. At the *Configure* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens and the *Switch* page displays with the *Beacon* tab selected
 - b. Click the *Online State* tab, then click *Set Offline*. The message **Your operations changes have been successfully activated** appears.
2. At the *Configure* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens with the *Switch* page displayed.

3. Click the *Feature Installation* tab. The *Operations* panel opens with the *Feature Installation* page displayed (Figure 2-24).

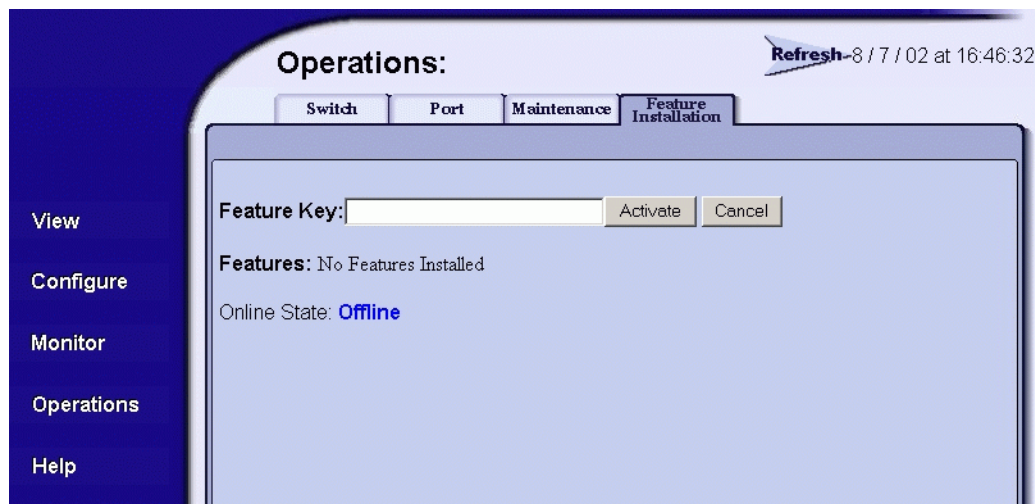


Figure 2-24 Operations Panel (Feature Installation Tab)

4. Type the PFE key and click *Activate*. The interface displays a confirmation page with a warning, stating this action overrides the current set of switch features.
5. Click *Activate* to activate the new PFE key. The switch performs an IPL when the key is activated.

NOTE: When *Activate* is selected, all current features are replaced with new features.

6. Set the switch online as follows:
 - a. At the *Configure* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens and the *Switch* page displays with the *Beacon* tab selected
 - b. Click the *Online State* tab, then click *Set Online*. The message **Your operations changes have been successfully activated** appears.

NOTE: PFE keys are encoded to work with the serial number of the installed switch only. Record the key to re-install the feature if required. If the switch fails and must be replaced, obtain new PFE keys from the

McDATA Solution Center (800-752-4572 or support@mcdata.com). Please have the serial numbers of the failed and replacement switches, and the old PFE key number or transaction code.

7. Go to [Task 21: Cable Fibre Channel Ports](#) on page 2-120.

Task 5: Configure Switch Network Information (Optional)

The switch is delivered with default network addresses as follows:

- **MAC address** - The media access control (MAC) address is programmed into FLASH memory on the control processor (CTP) card at the time of manufacture. The MAC address is unique for each switch, and should not be changed.
- **IP address** - The default IP address is **10.1.1.10**. If multiple switches are installed on the same LAN, each switch (and the management server) must have a unique IP address. One switch can use the default address, but the addresses of the remaining switches must be changed.

NOTE: If multiple switches and the management server are delivered in a McDATA Fabricenter equipment cabinet, all devices are configured with unique IP addresses that do not require change. The addresses require change only if multiple equipment cabinets are LAN-connected.

- **Subnet mask** - The default subnet mask is **255.0.0.0**. If the switch is installed on a complex public LAN with one or more routers, the address may require change.
- **Gateway address** - The default gateway address is **0.0.0.0**. If the switch is installed on a dedicated LAN with no connection through a router, the address does not require change. If the switch is installed on a public LAN (corporate intranet), the gateway address must be changed to the address of the corporate intranet's local router.

Verify the type of LAN installation with the customer's network administrator. If one switch is installed on a dedicated LAN, network addresses do not require change. Go to [Task 6: Unpack, Inspect, and Install the Management Server](#) on page 2-47.

If multiple switches are installed or a public LAN segment is used, network addresses must be changed to conform to the customer's LAN addressing scheme. The following tools are provided with the

switch or by installation or service personnel and are required to perform this task:

- A maintenance terminal (desktop or notebook PC) with:
 - The Microsoft Windows 98, Windows 2000, Windows Millennium Edition, Windows XP, or Windows NT 4.0 operating system.
 - RS-232 serial communication software (such as ProComm Plus or HyperTerminal). HyperTerminal is provided with Windows operating systems.
- An asynchronous RS-232 modem cable.

Perform the following steps to change a switch's IP address, subnet mask, or gateway address.

1. Using a Phillips screwdriver, remove the protective cap from the 9-pin maintenance port at the rear of the switch chassis. Connect one end of the RS-232 modem cable to the port.
2. Connect the other cable end to a 9-pin communication port (**COM1** or **COM2**) at the rear of the maintenance terminal PC.
3. Power on the maintenance terminal. After the PC powers on, the Windows desktop displays. If required, refer to operating instructions shipped with the PC.
4. At the Windows desktop, click *Start* at the left side of the task bar. The *Windows Workstation* menu displays.

NOTE: The following steps describe changing network addresses using HyperTerminal serial communication software.

5. At the *Windows Workstation* menu, sequentially select the *Programs* option, *Accessories* option, *Communications* option, and *HyperTerminal* option. The *Connection Description* dialog box displays ([Figure 2-25](#) on page 2-43).



Figure 2-25 Connection Description Dialog Box

6. Type **Sphereon 4500** in the *Name* field and click *OK*. The *Connect To* dialog box displays (Figure 2-26).



Figure 2-26 Connect To Dialog Box

7. Ensure the *Connect using* field displays **COM1** or **COM2** (depending on the serial communication port connection to the switch), and click *OK*. The *COMn Properties* dialog box displays, where *n* is 1 or 2 (Figure 2-27 on page 2-44).

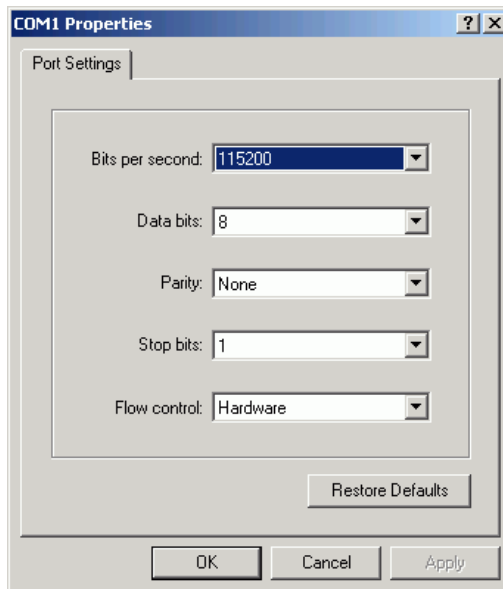


Figure 2-27 COMn Properties Dialog Box

8. Configure the *Port Settings* parameters as follows:

- *Bits per second* - **115200**.
- *Data bits* - **8**.
- *Parity* - **None**.
- *Stop bits* - **1**.
- *Flow control* - **Hardware** or **None**.

When the parameters are set, click **OK**. The *Sphereon 4500 - HyperTerminal* window displays.

9. At the **>** prompt, type the user-level password (the default is **password**) and press **Enter**. The password is case sensitive. The *Sphereon 4500 - HyperTerminal* window (Figure 2-28 on page 2-45) displays with software and hardware version information for the switch, and a **C >** prompt at the bottom of the window.

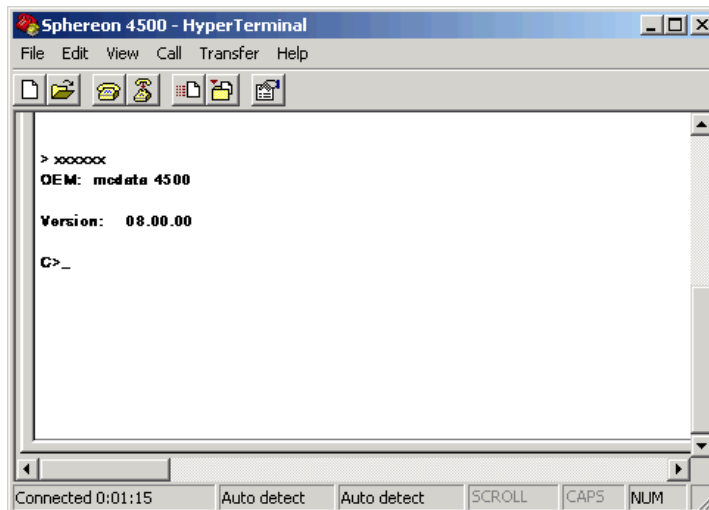


Figure 2-28 Sphereon 4500 - HyperTerminal Window

10. At the C > prompt, type the **ipconfig** command and press the **Enter** key. The *Sphereon 4500 - HyperTerminal* window displays with configuration information listed as follows:

- *MAC Address.*
- *IP Address* (default is **10.1.1.10**).
- *Subnet Mask* (default is **255.0.0.0**).
- *Gateway Address* (default is **0.0.0.0**).
- *Auto Negotiate.*
- *Speed.*
- *Duplex.*

Only the *IP Address*, *Subnet Mask*, and *Gateway Address* fields are configurable.

11. Change the IP address, subnet mask, and gateway address as directed by the customer's network administrator. To change the switch network addresses, type the following at the C > prompt and press the **Enter** key.

```
ipconfig xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy zzz.zzz.zzz.zzz
```

The IP address is always *xxx.xxx.xxx.xxx*, the subnet mask is always *yyy.yyy.yyy.yyy*, and the gateway address is always *zzz.zzz.zzz.zzz*, where the octets *xxx*, *yyy*, and *zzz* are decimals from zero through 255. If a network address is to remain unchanged, type the current address in the respective field.

When the new network addresses are configured at the switch, the message **Request completed OK** displays at the bottom of the *Sphereon 4500 - HyperTerminal* window.

12. Select the *Exit* option from the *File* pull-down menu to close the HyperTerminal application. A HyperTerminal message box appears (Figure 2-29):

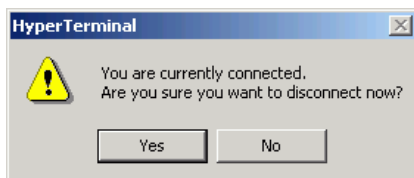


Figure 2-29 HyperTerminal Dialog Box (1)

13. Click *Yes*. A second HyperTerminal message box appears (Figure 2-30):

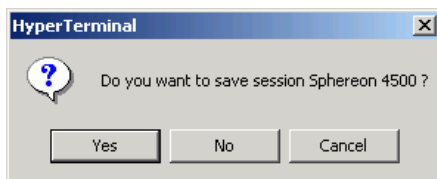


Figure 2-30 HyperTerminal Dialog Box (2)

14. Click *No* to exit and close the HyperTerminal application.
15. Power off the maintenance terminal:
 - a. Click *Start* at the left side of the task bar and select the *Shut Down* option. The *Shut Down Windows* dialog box appears.
 - b. At the *Shut Down Windows* dialog box, select the *Shut down* option from the list box and click *OK* to power off the PC.

16. Disconnect the RS-232 modem cable from the switch and the maintenance terminal. Replace the protective cap over the maintenance port.
17. At the switch front panel, press and hold the **IML/RESET** button for ten seconds. The switch performs a POR.
18. Connect the switch to the customer-supplied Ethernet LAN segment, or McDATA Ethernet hub. To connect the desktop or rack-mounted (customer-supplied) switch to the Internet or Ethernet LAN segment:
 - a. Connect one end of the Ethernet patch cable (supplied with the switch) to the RJ-45 connector (labelled **10/100**) on the left front of the switch chassis.
 - b. Connect the remaining end of the Ethernet cable. Perform one of the following steps:
 - If the switch is to be installed on a customer-supplied LAN segment, connect the cable to the LAN as directed by the customer's network administrator.
 - If the switch is to be installed on the McDATA Ethernet hub, connect the cable to any available hub port.
19. Perform one of the following steps:
 - If the switch is delivered separately from the management server, go to [Task 6: Unpack, Inspect, and Install the Management Server](#) below.
 - If the switch is delivered as part of an FC-512 Fabriccenter equipment cabinet, go to [Task 7: Configure Server Password and Network Addresses](#) on page 2-51.

Task 6: Unpack, Inspect, and Install the Management Server

The management server is a 1U high, rack-mount unit with the SAN management (SANavigator 4.0 or EFCM 8.0) and Sphereon 4500 Element Manager applications installed. The applications provide a graphical user interface (GUI) for operating and managing the switch and other McDATA products. The management server also includes a TightVNC Viewer Version 1.2.7 client-server software control package that provides remote network access (through a standard web browser) to the server desktop. For information about the TightVNC Viewer, refer to www.tightvnc.com.

NOTE: The management server and related applications provide a GUI to monitor and manage McDATA products, and are a dedicated hardware and software solution that should not be used for other tasks. McDATA tests applications installed on the management server, but does not compatibility test other third-party software. Modifications to the management server hardware or installation of additional software (including patches or service packs) may interfere with normal operation.

Unpack, inspect, and install the management server as follows:

1. Inspect the shipping container for damage caused during transit. If a container is damaged, ensure a representative from the freight carrier is present when the container is opened.
2. Unpack the shipping container and inspect each item for damage. Ensure the packaged items correspond to the items listed on the enclosed bill of materials.
3. If any items are damaged or missing, customers should call the toll-free telephone number printed on the service label attached to the bottom of the server.
4. Perform one of the following:
 - For a desktop installation, position the management server on a table or desktop as directed by the customer. Ensure a grounded AC electrical outlet is available.
 - For a cabinet installation, open the rack-mount kit and inspect the contents. Refer to the enclosed bill of materials and verify all parts are delivered.

Install the management server in the equipment cabinet. Refer to the *1U Server Rack-Mount Kit Installation Instructions* (958-000310) for guidance.
5. Connect the management server to the customer-supplied Ethernet LAN segment or McDATA-supplied Ethernet hub (private LAN interface). To connect the server:
 - a. As shown in [Figure 2-31](#) on page 2-49, connect one end of the Ethernet patch cable (supplied with the management server) to the right RJ-45 adapter (**LAN 2**) at the rear of the server.

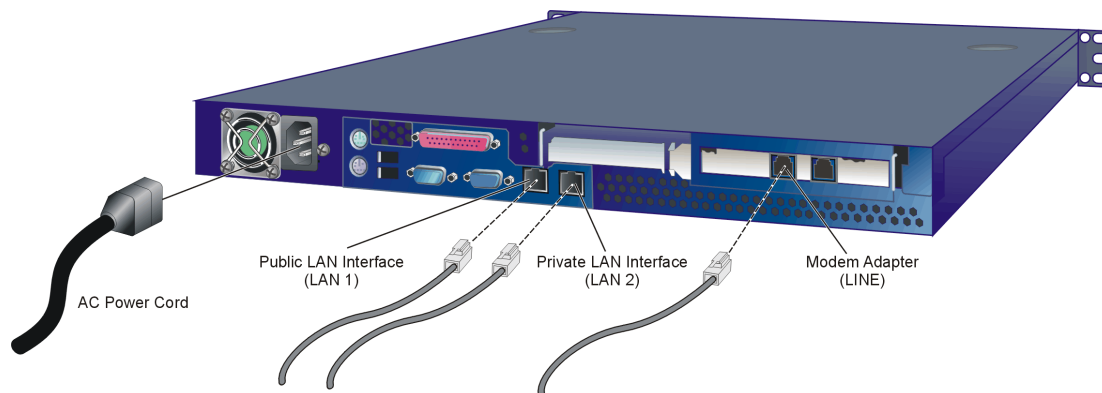


Figure 2-31 1U Management Server Connections

- b. Connect the remaining end of the Ethernet cable to the LAN as follows:
 - If the server is installed on a customer-supplied LAN segment, connect the cable to the LAN as directed by the customer's network administrator.
 - If the server is installed on the McDATA-supplied Ethernet hub, connect the cable to any available hub port.
 6. If required, connect the management server to the customer's corporate intranet (public LAN interface). To connect the server:
 - a. As shown in [Figure 2-31](#), connect one end of a customer-supplied Ethernet patch cable to the left RJ-45 adapter (**LAN 1**) at the rear of the server.
 - b. Connect the remaining end of the Ethernet cable to the corporate intranet as directed by the customer's network administrator.
 7. As shown in [Figure 2-31](#), connect the 20-foot phone cord to the left RJ-11 adapter (**LINE**) at the rear of the server and to a facility telephone connection.
 8. As shown in [Figure 2-31](#), connect the AC power cord to the server and to a facility power source or rack power strip that provides single-phase, 90 to 264 VAC current.
 9. When the power cord is connected, the server powers on and performs power-on self-tests (POSTs). During POSTs:

- a. The green liquid crystal display (LCD) panel illuminates.
- b. The green hard disk drive (**HDD**) LED blinks momentarily, and processor speed and random-access memory information display momentarily at the LCD panel.
- c. After a few seconds, the LCD panel displays the following message pertaining to boot sequence selection ([Figure 2-32](#)):



Boot from LAN?
Press <Enter>

Figure 2-32 LCD Panel During Boot Sequence

- d. Ignore the message. After ten seconds, the server performs the boot sequence from the basic input/output system (BIOS). After successful boot and POST completion, the LCD panel displays a **Welcome!!** message.
- e. The server then continuously cycles through and displays the following operational information at the LCD panel:
 - Host name.
 - System date and time.
 - LAN 1 and LAN 2 IP addresses.
 - Fan 1, fan 2, fan 3, and fan 4 rotational speed.
 - Central processing unit (CPU) temperature.
 - Hard disk capacity.
 - Virtual and physical memory capacity.
10. If a POST error or other malfunction occurs, go to [MAP 0000: Start MAP](#) on page 3-6 to isolate the problem.
11. Press the left edge (**PUSH** label) of the LCD panel to disengage the panel and expose the CD-RW drive.
12. Insert a blank rewritable CD into the CD-RW drive and close the LCD panel.

Task 7: Configure Server Password and Network Addresses

Verify the type of LAN installation with the customer's network administrator. If the management server or Fabriccenter equipment cabinet is installed on a dedicated LAN, network information does not require change. Change the default password for the server's LCD panel (if required by the customer), then go to [Task 8: Configure Management Server Information](#) on page 2-55.

If the management server or Fabriccenter equipment cabinet is installed on a public LAN segment, the default password for the server's LCD panel and the following transmission control protocol internet protocol (TCP/IP) network information must be changed to conform to the customer's LAN addressing scheme:

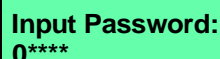
- IP address.
- Subnet mask.

NOTE: At some customer installations, TCP/IP addresses for the management server may be allocated automatically using dynamic host configuration protocol (DHCP).

Configure Password

To configure a new LCD panel password:

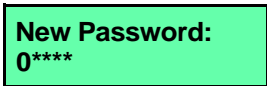
1. At the management server's LCD panel, press **ENTER**. The **Welcome!!** or operational information message changes to the following ([Figure 2-33](#)):



Input Password:
0****

Figure 2-33 LCD Panel (Password Entry)

2. Using the **▲** button to increment a digit, the **▼** button to decrement a digit, the **◀** button to move the cursor left, and the **▶** button to move the cursor right, input the default password (9999), and press **ENTER**. The **LAN 1 Setting??** message appears at the LCD panel.
3. Press the **▼** button several times until the **Change Password?** option appears at the LCD panel, then press **ENTER**. The following message appears ([Figure 2-34](#) on page 2-52):



New Password:
0****

Figure 2-34 LCD Panel (New Password)

4. Use the arrow keys as described in [step 2](#) to input a new 4-digit numeric password, then press **ENTER**. The following message appears ([Figure 2-35](#)):



Save Change?
Yes, Save !!

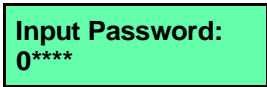
Figure 2-35 LCD Panel (Save Change)

5. Press **ENTER**. A **Wait a moment!** message appears at the LCD panel, the LCD panel returns to the **LAN 1 Setting??** message, and the password changes.

Configure Private LAN Addresses

To configure TCP/IP network information for the private LAN connection (LAN 2):

1. At the management server's LCD panel, press **ENTER**. The **Welcome!!** or operational information message changes to the following ([Figure 2-36](#)):



Input Password:
0****

Figure 2-36 LCD Panel (Password Entry)

2. Using the ▲ button to increment a digit, the ▼ button to decrement a digit, the ◀ button to move the cursor left, and the ▶ button to move the cursor right, input the default or changed password, and press **ENTER**. The **LAN 1 Setting??** message appears at the LCD panel.
3. Press the ▼ button. The **LAN 2 Setting??** message appears at the LCD panel. Press **ENTER** and the following message appears ([Figure 2-37](#) on page 2-53) with the default IP address of **10.1.1.1**.



Input IP:
010.001.001.001

Figure 2-37 LCD Panel (LAN 2 IP Address)

4. Use the arrow keys as described in [step 2](#) to input a new IP address, then press **ENTER**. The following message appears ([Figure 2-38](#)):



Save Change?
Yes, Save !!

Figure 2-38 LCD Panel (Save Change)

5. Press **ENTER**. The LAN 2 IP address changes and the following message appears ([Figure 2-39](#) on page 2-53) with the default subnet mask of 255.0.0.0.



Input Netmask:
255.000.000.000

Figure 2-39 LCD Panel (LAN 2 Subnet Mask)

6. Use the arrow keys as described in [step 2](#) to input a new subnet mask, then press **ENTER**. The following message appears ([Figure 2-40](#)):



Save Change?
Yes, Save !!

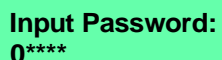
Figure 2-40 LCD Panel (Save Change)

7. Press **ENTER**. A **Wait a moment!** message appears at the LCD panel, the LCD panel returns to the **LAN 1 Setting??** message, and the LAN 2 subnet mask changes.
8. Record the private LAN IP address and subnet mask for reference if the management server hard drive fails and must be restored.

Configure Public LAN Addresses (Optional)

To optionally configure TCP/IP network information for the public LAN connection (LAN 1):


1. At the management server's LCD panel, press **ENTER**. The **Welcome!!** or operational information message changes to the following (Figure 2-41):



Input Password:
0****

Figure 2-41 LCD Panel (Password Entry)

2. Using the ▲ button to increment a digit, the ▼ button to decrement a digit, the ◀ button to move the cursor left, and the ▶ button to move the cursor right, input the default or changed password, and press **ENTER**. The **LAN 1 Setting??** message appears at the LCD panel.
3. Press **ENTER** and the following message appears (Figure 2-42) with the default IP address of **192.168.0.1**.



Input IP:
192.168.000.001

Figure 2-42 LCD Panel (LAN 1 IP Address)

4. Use the arrow keys as described in [step 2](#) to input a new IP address, then press **ENTER**. The following message appears (Figure 2-43):



Save Change?
Yes, Save !!

Figure 2-43 LCD Panel (Save Change)

5. Press **ENTER**. The LAN 1 IP address changes and the following message appears (Figure 2-44 on page 2-55) with the default subnet mask of **255.0.0.0**.



Input Netmask:
255.000.000.000

Figure 2-44 LCD Panel (LAN 1 Subnet Mask)

6. Use the arrow keys as described in [step 2](#) to input a new subnet mask, then press **ENTER**. The following message appears ([Figure 2-45](#)):



Save Change?
Yes, Save !!

Figure 2-45 LCD Panel (Save Change)

7. Press **ENTER**. A **Wait a moment!** message appears at the LCD panel, the LCD panel returns to the **LAN 1 Setting??** message, and the LAN 1 subnet mask changes.
8. Record the public LAN IP address and subnet mask for reference if the management server hard drive fails and must be restored.

Task 8: Configure Management Server Information

Configure the computer name and workgroup name for the management server. Configure these parameters from the server's Windows 2000 operating system, using a LAN-attached PC with standard web browser.

If required, change the management server's gateway addresses and domain name system (DNS) server IP addresses to conform to the customer's LAN addressing scheme. The gateway addresses are the addresses of the local router for the corporate intranet.

Access the Management Server Desktop

To login and access the management server desktop:

1. Ensure the management server and a browser-capable PC are connected through an Ethernet LAN segment. At the PC, launch the browser application (Netscape Navigator or Internet Explorer).

2. At the PC browser, enter the LAN 2 IP address of the management server, followed by :5800, as the Internet uniform resource locator (URL). Enter the URL in the following format:

http://xxx.xxx.xxx.xxx:5800

Where *xxx.xxx.xxx.xxx* is the default IP address of **10.1.1.1** or the IP address configured while performing *Task 7: Configure Server Password and Network Addresses* on page 2-51. The VNC Authentication screen displays (Figure 2-46).

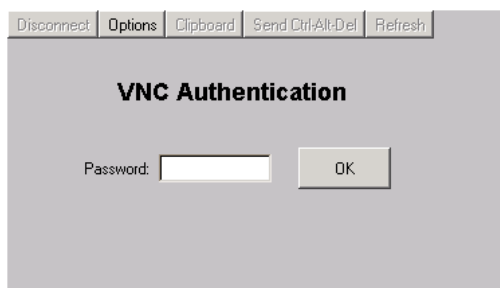


Figure 2-46 VNC Authentication Screen

3. Type the default password and click OK. The *Welcome to Windows* dialog box displays (Figure 2-47).

NOTE: The default TightVNC viewer password is **password**.

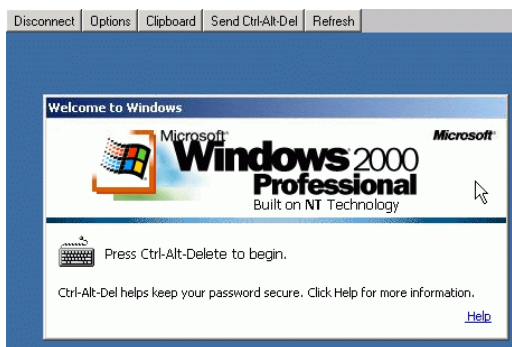


Figure 2-47 Welcome to Windows Dialog Box

4. Click the **Send Ctrl-Alt-Del** button at the top of the window to log on to the management server desktop. The *Log On to Windows* dialog box displays (Figure 2-48).

NOTE: Do not simultaneously press the **Ctrl**, **Alt**, and **Delete** keys. This action logs the user on to the browser-capable PC, not the rack-mount management server.



Figure 2-48 Log On to Windows Dialog Box

5. Type the default Windows 2000 user name and password and click OK. The management server's Windows 2000 desktop opens and the *SANavigator Log In* or *EFCM Log In* dialog box displays (Figure 2-49).

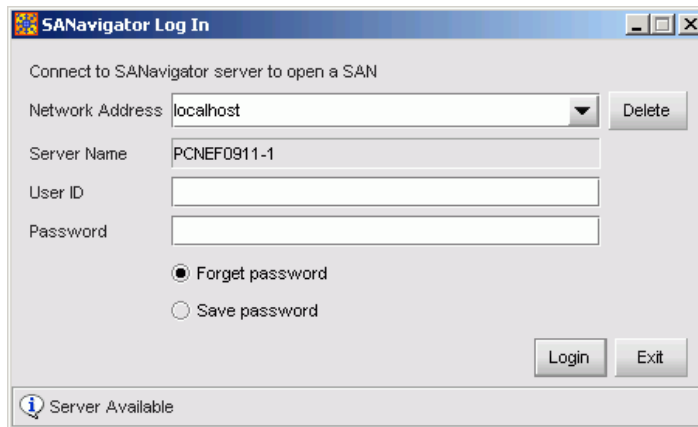


Figure 2-49 SANavigator Log In or EFCM Log In Dialog Box

NOTE: The default Windows 2000 user name is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

Configure Management Server Names

To configure the management server name and workgroup name:

1. At the Windows 2000 desktop, click *Start* at the left side of the task bar (bottom of the desktop), then select *Settings*, then *Control Panel*. The *Control Panel* window displays (Figure 2-50).

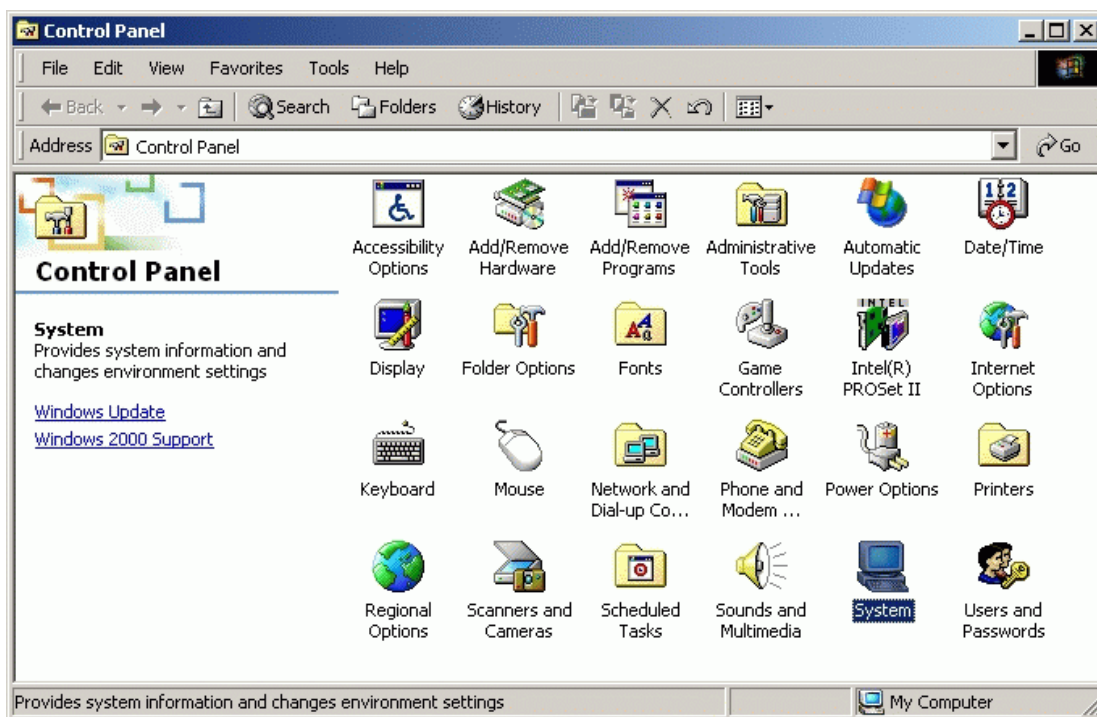


Figure 2-50 Control Panel Window

2. Double-click the *System* icon. The *System Properties* dialog box displays with the *General* tab selected as the default.
3. Click the *Network Identification* tab. The *System Properties* dialog box displays with the *Network Identification* tab selected (Figure 2-51 on page 2-59).

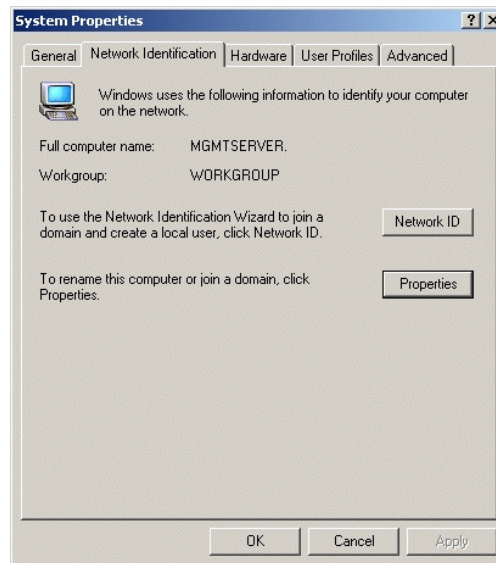


Figure 2-51 System Properties Dialog Box (Network Identification Tab)

4. Click *Properties*. The *Identification Changes* dialog box displays (Figure 2-52).

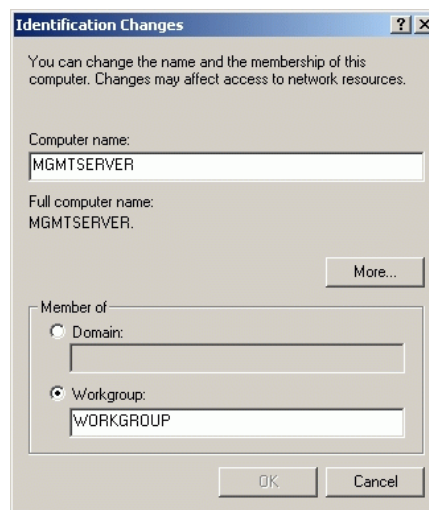


Figure 2-52 Identification Changes Dialog Box

5. At the *Computer Name* field, change the name to **MGMTSERVER**, at the *Workgroup* field, change the name to **WORKGROUP**, then click OK. The dialog box closes.
6. Record the computer and workgroup names for reference if the management server hard drive fails and must be restored.
7. At the *System Properties* dialog box, click OK to close the dialog box and return to the *Control Panel* window.
8. Click close (X) at the upper right corner of the *Control Panel* window to return to the Windows 2000 desktop.

Configure Gateway and DNS Server Addresses

To configure gateway addresses and DNS server IP addresses for the private LAN connection (LAN 2) and optional public LAN connection (LAN 1):

1. At the Windows 2000 desktop, click *Start* at the left side of the task bar, then select *Settings*, then *Control Panel*. The *Control Panel* window displays (Figure 2-50 on page 2-58).
2. Double-click the *Network and Dial-up Connections* icon. The *Network and Dial-up Connections* window displays (Figure 2-53).

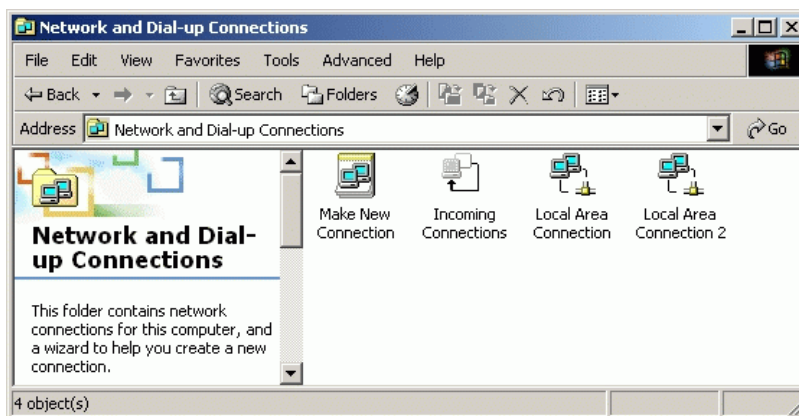


Figure 2-53 Network and Dial-up Connections Window

3. To configure addresses for the private LAN connection (LAN 2), double-click the *Local Area Connection 2* icon. The *Local Area Connection 2 Status* dialog box displays (Figure 2-54 on page 2-61).

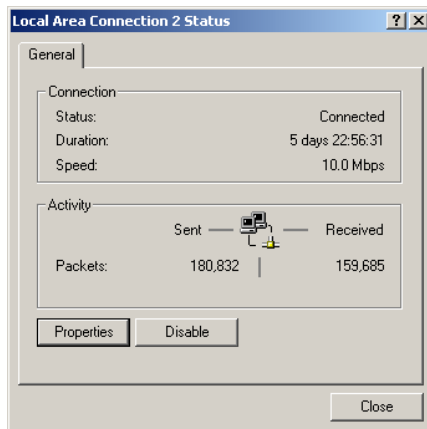


Figure 2-54 Local Area Connection 2 Status Dialog Box

4. Click *Properties*. The *Local Area Connection 2 Properties* dialog box displays (Figure 2-55).

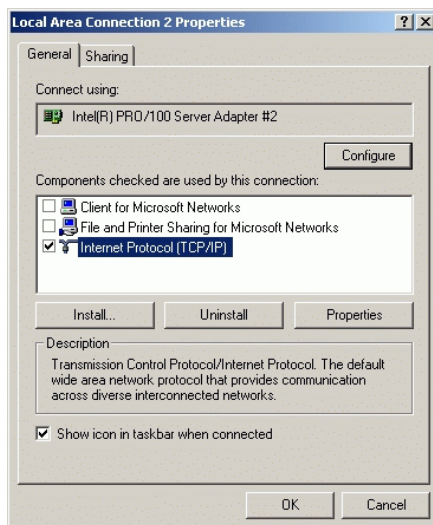


Figure 2-55 Local Area Connection 2 Properties Dialog Box

5. Double-click the *Internet Protocol (TCP/IP)* entry. The *Internet Protocol (TCP/IP) Properties* dialog box displays (Figure 2-56 on page 2-62).

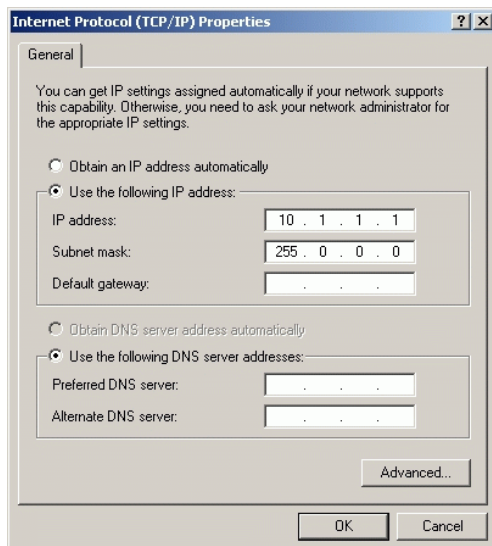


Figure 2-56 Internet Protocol (TCP/IP) Properties Dialog Box

6. The *Use the following IP address* radio button is enabled and the *IP address* and *Subnet mask* fields display network information configured while performing [Task 7: Configure Server Password and Network Addresses](#) on page 2-51.
7. At the *Default gateway* field, enter the gateway address obtained from the customer's network administrator.
8. Select (enable) the *Use the following DNS server addresses* radio button. At the *Preferred DNS server* field, enter the DNS server IP address obtained from the customer's network administrator, then click OK to apply the changes and close the dialog box.
9. Click OK to close the *Local Area Connection 2 Properties* dialog box.
10. Record the changed gateway and DNS server addresses for reference if the management server hard drive fails and must be restored.
11. To optionally configure addresses for the public LAN connection (LAN 1), double-click the *Local Area Connection 1* icon and repeat [step 3](#) through [step 10](#) of this procedure.
12. Click close (X) at the upper right corner of the *Network and Dial-up Connections* window to return to the Windows 2000 desktop.

13. Reboot the management server:
 - a. At the Windows 2000 desktop, click *Start* at the left side of the task bar (bottom of the desktop), then select *Shut down*. The *Shut Down Windows* dialog box appears.
 - b. At the *Shut Down Windows* dialog box, select the *Restart* option and click *OK* to reboot the server.
 - c. Perform [Access the Management Server Desktop](#) on page 2-55.

Task 9: Configure Windows 2000 Users

Configure password access for all authorized Windows 2000 users of the management server. It is also recommended to change the default administrator password. To configure users:

1. At the Windows 2000 desktop, click *Start* at the left side of the task bar, then select *Settings*, then *Control Panel*. The *Control Panel* window displays ([Figure 2-50](#) on page 2-58).
2. Double-click the *Users and Passwords* icon. The *Users and Passwords* dialog box displays ([Figure 2-57](#)).

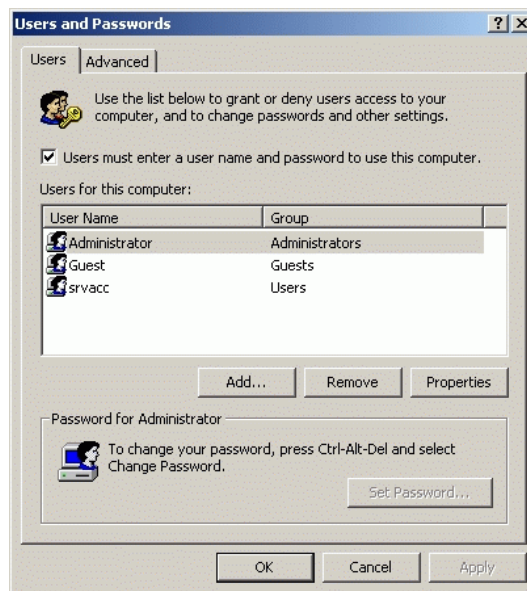


Figure 2-57 Users and Passwords Dialog Box

Change Default Administrator Password

3. The *Guest* user name is a built-in account in the Windows 2000 operating system and cannot be deleted. The *svracc* account is for field service users and must not be modified or deleted.

To change the administrator password from the default (**password**) to a customer-specified password:

1. Click the **Send Ctrl-Alt-Del** button at the top of the window surrounding the *Users and Passwords* dialog box. The *Windows Security* dialog box displays ([Figure 2-58](#)).

NOTE: Do not simultaneously press the **Ctrl**, **Alt**, and **Delete** keys. This action controls the browser-capable PC, not the rack-mount management server.



Figure 2-58 Windows Security Dialog Box

2. Click *Change Password*. The *Change Password* dialog box displays ([Figure 2-59](#) on page 2-65).



Figure 2-59 Change Password Dialog Box

3. At the *Old Password* field, type the old password. At the *New Password* and *Confirm New Password* fields, type the new password.

NOTE: The *New Password* and *Confirm New Password* fields are case-sensitive.

4. Click *OK*. The default administrator password changes and the *Change Password* dialog box closes.
5. Click *Cancel* at the *Windows Security* dialog box to return to the *Users and Passwords* dialog box.

Add a New User

To set up a new Windows 2000 user:

1. At the *Users and Passwords* dialog box, click *Add*. The first window of the *Add New User* wizard displays (Figure 2-60 on page 2-66).

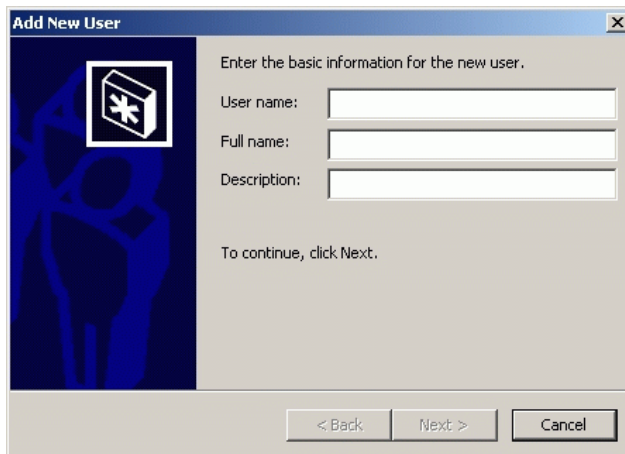
The image shows the first window of the 'Add New User' wizard. The window has a title bar with the text 'Add New User' and a close button. On the left side, there is a blue background with a white icon of a box with a plus sign. The main area contains the text 'Enter the basic information for the new user.' followed by three input fields: 'User name:', 'Full name:', and 'Description:'. Below these fields, it says 'To continue, click Next.' At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Figure 2-60 Add New User Wizard (First Window)

2. Type the appropriate new user information in the *User name*, *Full name*, and *Description* fields, then click *Next*. The second window of the *Add New User* wizard displays ([Figure 2-61](#)).

The image shows the second window of the 'Add New User' wizard. The window has a title bar with the text 'Add New User' and a close button. On the left side, there is a blue background with a white icon of a box with a plus sign. The main area contains the text 'Type and confirm a password for this user.' followed by two input fields: 'Password:' and 'Confirm password:'. Below these fields, it says 'To continue, click Next.' At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Figure 2-61 Add New User Wizard (Second Window)

3. Type the new user's password in the *Password* and *Confirm password* fields, then click *Next*. The third window of the *Add New User* wizard displays (Figure 2-62).

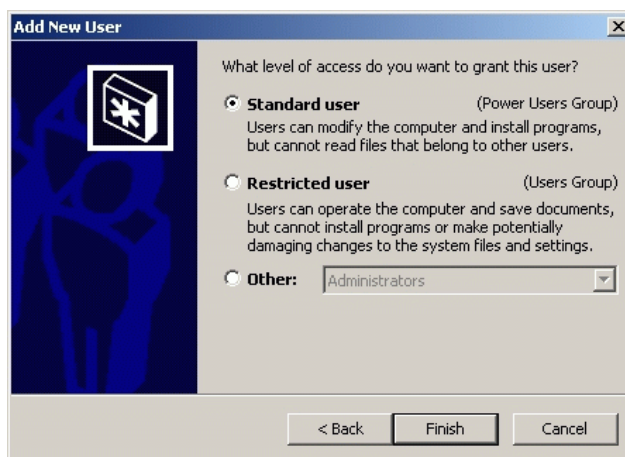


Figure 2-62 Add New User Wizard (Third Window)

4. Based on the level of access to be granted, select the *Standard user*, *Restricted user*, or *Other* radio button. If the *Other* radio button is selected, choose the type of access from the adjacent list box.
5. Click *Finish*. The new user information is added and the wizard closes. Record the user information for reference if the management server hard drive fails and must be restored.
6. If no other users are to be added, click *OK* to close the *Users and Passwords* dialog box.
7. Click close (X) at the upper right corner of the *Control Panel* window to return to the Windows 2000 desktop.

Change User Properties

To change an existing user's properties:

1. At the *Users and Passwords* dialog box, highlight the user (*srvacc*, for example) at the *Users for this computer* field and click *Properties*. The *MGMTSERVER\srvacc Properties* dialog box displays with the *General* tab selected (Figure 2-63 on page 2-68).

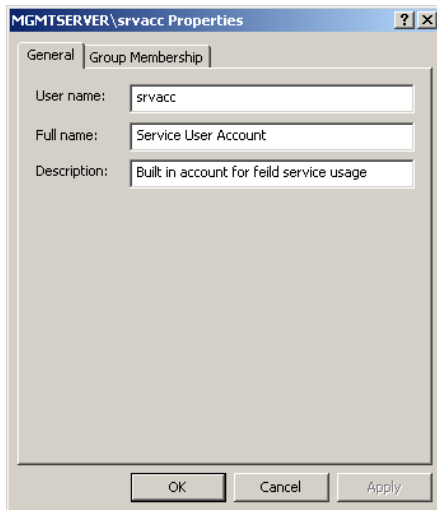


Figure 2-63 MGMTSERVER\srvacc Properties Dialog Box (General Tab)

2. Type the appropriate new user information in the *User name*, *Full name*, and *Description* fields, then click the *Group Membership* tab. The *MGMTSERVER\srvacc Properties* dialog box displays with the *Group Membership* tab selected (Figure 2-64).

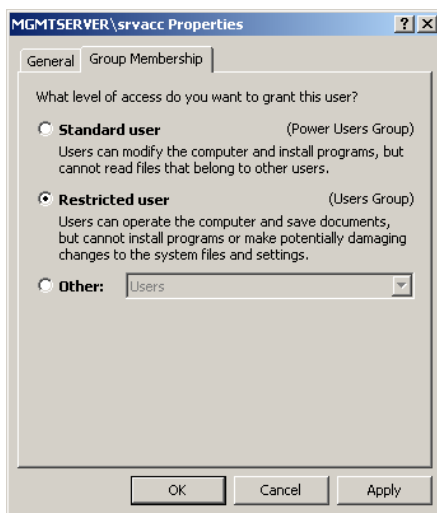


Figure 2-64 MGMTSERVER\srvacc Properties Dialog Box (Group Membership Tab)

3. Based on the level of access to be changed, select the *Standard user*, *Restricted user*, or *Other* radio button. If the *Other* radio button is selected, choose the type of access from the adjacent list box.
4. Click *OK*. The new user information is added and the *MGMTSERVER\srvacc Properties* dialog box closes. Record the user information for reference if the management server hard drive fails and must be restored.
5. If no other users are to be changed, click *OK* to close the *Users and Passwords* dialog box.
6. Click close (X) at the upper right corner of the *Control Panel* window to return to the Windows 2000 desktop.

Task 10: Set Management Server Date and Time

The SAN Management application's audit and event logs are stamped with the date and time from the management server. The switch's system clock is synchronized with date and time of the management server by default. To set the server date and time:

1. At the Windows 2000 desktop, click *Start* at the left side of the task bar, then select *Settings*, then *Control Panel*. The *Control Panel* window displays (Figure 2-50 on page 2-58).
2. Double-click the *Date/Time* icon. The *Date/Time Properties* dialog box displays with the *Date & Time* page open (Figure 2-65).

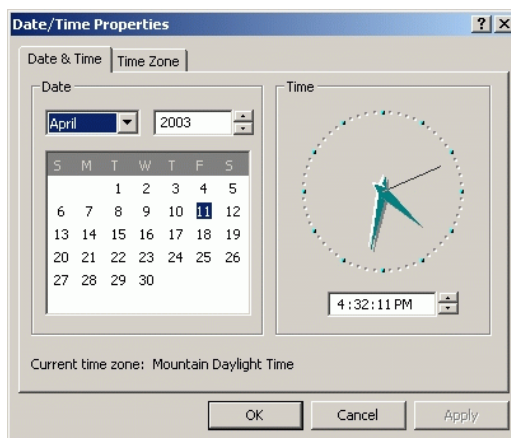


Figure 2-65 Date/Time Properties Dialog Box (Date & Time Tab)

NOTE: The *Time Zone* field must be set before the *Date & Time* field.

3. Click the *Time Zone* tab. The *Date/Time Properties* dialog box displays with the *Time Zone* page open (Figure 2-66).

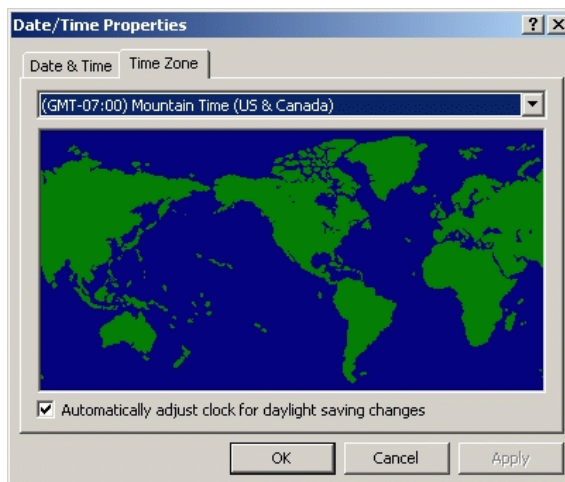


Figure 2-66 Date/Time Properties Dialog Box (Time Zone Tab)

4. To change the time zone:
 - a. Select the appropriate time zone from the drop-down list at the top of the dialog box.
 - b. If instructed by the customer's system administrator, select the *Automatically adjust clock for daylight saving changes* check box.
 - c. Click *Apply*. Record time zone and daylight savings information for reference if the management server hard drive fails and must be restored.
5. Click the *Date & Time* tab. The *Date/Time Properties* dialog box displays with the *Date & Time* page open.
6. To change the date and time:
 - a. Select the month from the drop-down list under *Date*.
 - b. Click the up or down arrow adjacent to the year field and select the desired year.
 - c. Click the day on the calendar to select the desired date.

- d. Click in the time field and enter the desired time, then click the adjacent up or down arrow and select *AM* or *PM*.
 - e. Click *Apply*. Record date and time information for reference if the management server hard drive fails and must be restored.
7. Click *OK* to close the *Date/Time Properties* dialog box.
 8. Click close (X) at the upper right corner of the *Control Panel* window to return to the Windows 2000 desktop.

Task 11: Configure the Call-Home Feature (Optional)

The management server has an optional call-home feature that provides automatic dial-out through the internal modem to a service support facility to report switch problems. The problem is logged into the support facility's tracking system for resolution. To configure the call-home feature:

1. There are two jacks on the management server's internal modem: one for the call-home connection (**LINE**), and the other for a telephone (**PHONE**). Ensure a telephone cable is routed and connected to the **LINE** jack at the rear of the management server (connected while performing [Task 6: Unpack, Inspect, and Install the Management Server](#) on page 2-47).
2. At the Windows 2000 desktop, double-click the *CallHome Configuration* icon. The *Call Home Configuration* dialog box displays ([Figure 2-67](#)).

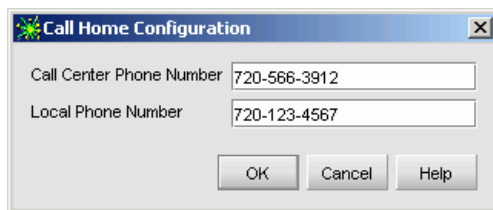


Figure 2-67 Call Home Configuration Dialog Box

3. At the *Call Center Phone Number* field, enter the telephone number for the McDATA Solution Center (720-566-3912). Include necessary information, such as the country code, area code, or any prefix required to access a telephone line outside the facility.
4. At the *Local Phone Number* field, enter the telephone number for access to the local server. Include necessary information such as the country code or area code.
5. Click *OK* to save the configured telephone numbers and close the dialog box.

Task 12: Assign User Names and Passwords

In addition to password access for the Windows 2000 operating system, users must be configured for access to the SAN management application. To assign user names and passwords:

1. At the Windows 2000 desktop, the *SANavigator Log In* or *EFCM Log In* dialog box displays (Figure 2-49 on page 2-57). The dialog box was opened when performing [Task 8: Configure Management Server Information](#) on page 2-55.
2. Type the SAN management application default user ID and password and select a server or IP address from the *Network Address* drop-down list.

NOTE: The default SAN management application user ID is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

3. Click *Login*. The application opens and the SANavigator or EFCM main window appears (Figure 2-68 on page 2-73).

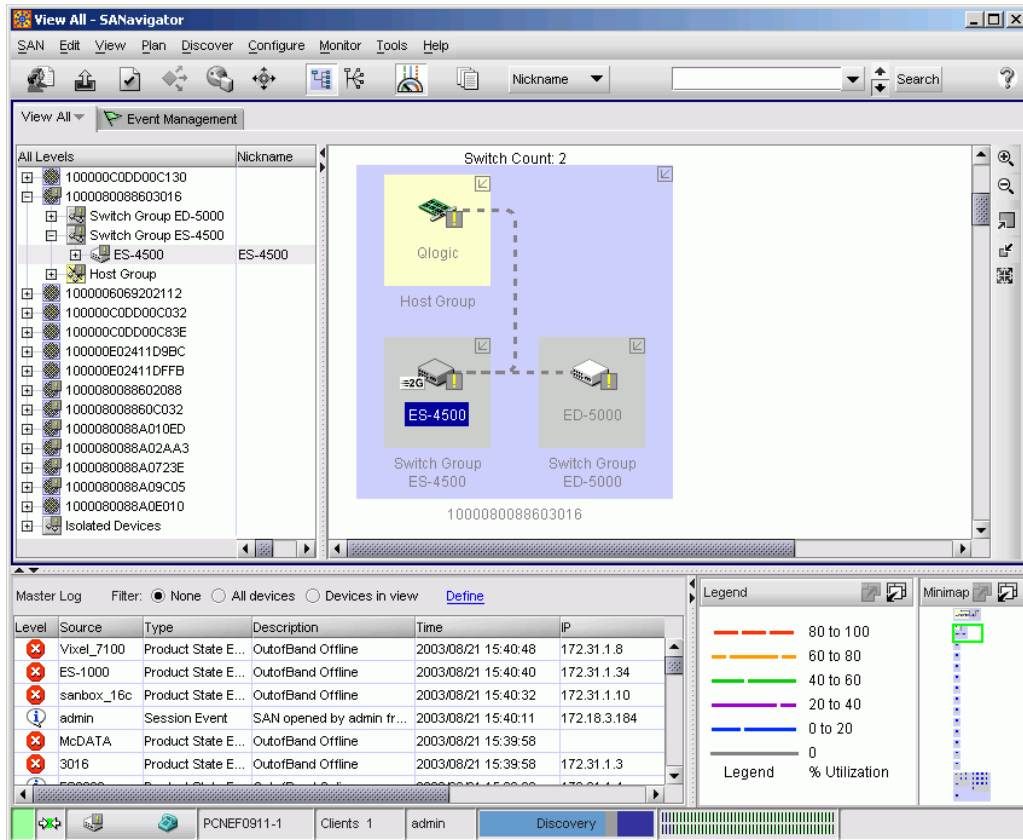


Figure 2-68 Main Window (SANavigator or EFCM)

4. Select *Users* from the SAN menu. The *SANavigator Server Users* or *EFCM 8 Server Users* dialog box displays (Figure 2-69 on page 2-74).

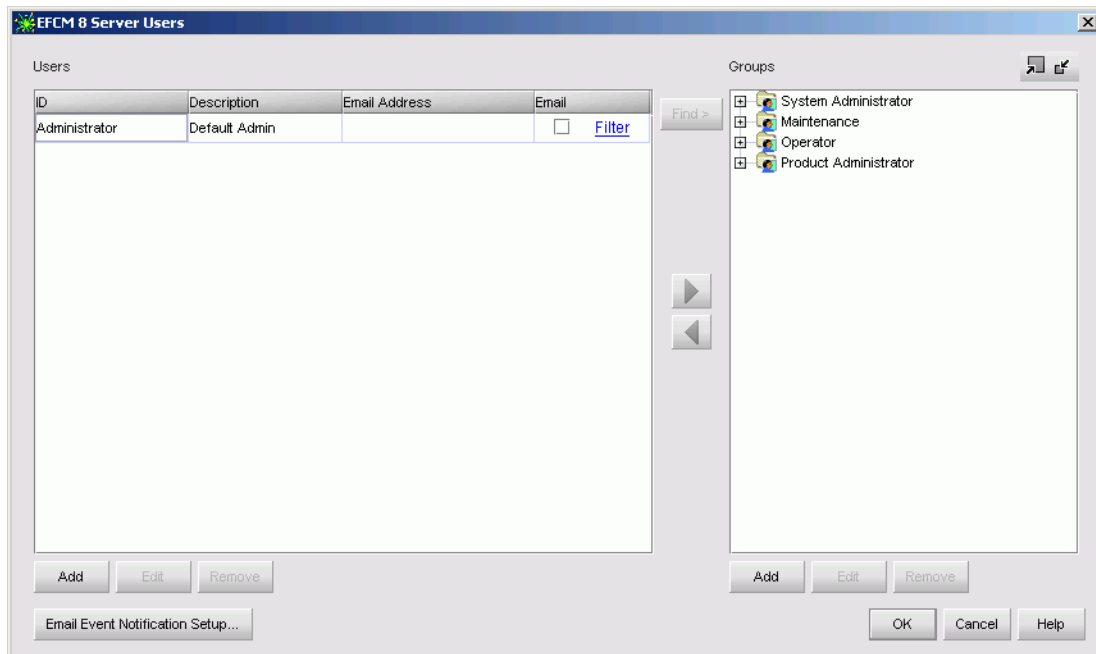


Figure 2-69 SANavigator or EFCM 8 Server Users Dialog Box

5. Click *Add*. The *Add User* dialog box displays ([Figure 2-70](#)).

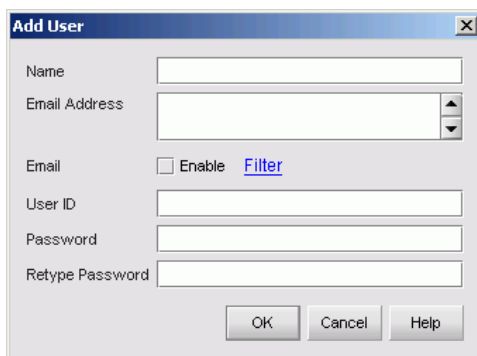


Figure 2-70 Add User Dialog Box

6. Enter information in fields as directed by the customer:
 - **Name** - click in this field and type a new user name up to 16 alphanumeric characters in length. Control characters and spaces are not valid. The user name is case-sensitive.
 - **Email Address** - click in this field and type one or more new user e-mail addresses. Separate multiple addresses with a semicolon.
 - **User ID** - click in this field and type a unique user ID for the new user.
 - **Password** - click in this field and type a password up to 16 alphanumeric characters in length. Control characters and spaces are not valid. The password is case-sensitive.
 - **Retype Password** - to confirm the password is entered correctly, click in this field and enter the password exactly as in the *Password* field. If an incorrect keystroke is entered, use the **Backspace** key to delete individual letters or select the entire entry and use the **Delete** key.
7. To enable e-mail notification for the new user, select (click) the *Enable* check box. An unchecked box indicates e-mail notification is not enabled.
8. To configure event types for which e-mail notification is sent, select (click) the *Filter* link. The *Define Filter* dialog box displays. For instructions on defining event filters, refer to the *SANavigator Software Release 4.0 User Manual* (621-000013) or *EFC Manager Software Release 8.0 User Manual* (620-000170).
9. Click *OK* to accept the information and close the dialog box.
10. Repeat [step 5](#) through [step 9](#) as required to assign multiple user names and passwords.
11. When finished, click *OK* at the *SANavigator Server Users* or *EFCM 8 Server Users* dialog box to return to the *SANavigator* or *EFCM* main window.

Task 13: Configure the Switch to the Management Application

To manage a new switch, it must be identified to and discovered by the SAN management application. To identify the new switch:

1. At the SAN management application (SANavigator or EFCM main window), select the *Setup* option from the *Discover* menu. The *Discover Setup* dialog box displays (Figure 2-71).

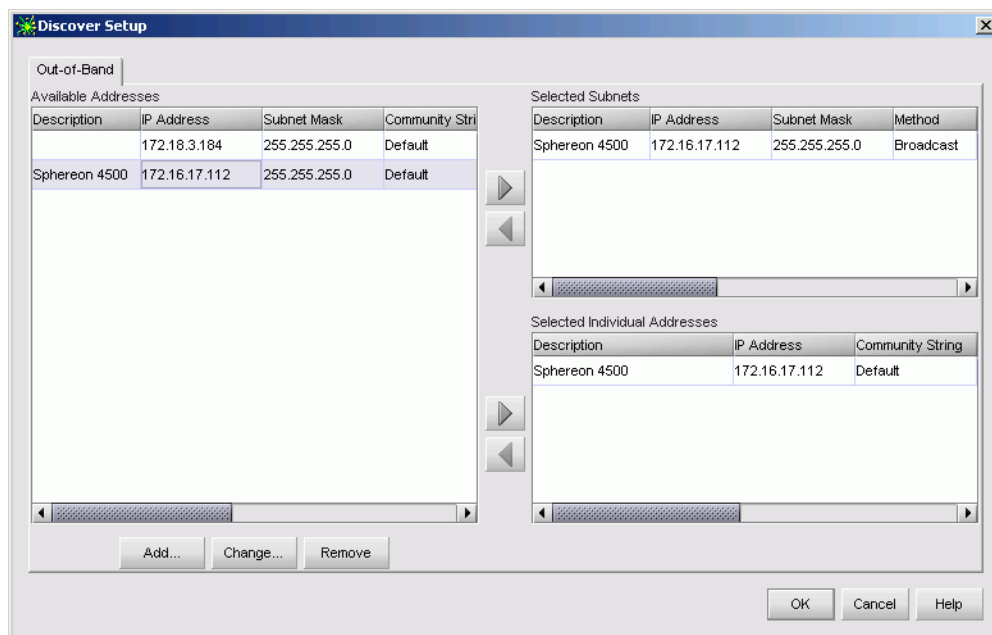


Figure 2-71 Discover Setup Dialog Box

2. Click *Add*. The *Domain Information* dialog box displays with the *IP Address* page open by default (Figure 2-72 on page 2-77).

The image shows a Windows-style dialog box titled "Domain Information". It has three tabs: "IP Address" (selected), "Community Strings", and "Device Access". The "IP Address" tab contains several input fields: "Description" with the text "Sphereon 4500", "IP Address" with "172.16.17.112", and "Subnet Mask" with "255.255.255.0". Below these is a section titled "Data Source for Domain" containing three radio buttons: "Use auto detection" (which is selected), "Use the server", and "Use a specific RDC". Below the radio buttons is a text field labeled "IP address of RDC". At the bottom of the dialog is a section titled "Add Multiple" containing a checkbox labeled "Generate a sequence of IP addresses". Below this checkbox is the text "Use the IP above as the first address" and a text field labeled "Last IP". At the very bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

Figure 2-72 Domain Information Dialog Box (IP Address Page)

3. Type a switch description (**Sphereon 4500**, for example) in the *Description* field.
4. Type the switch IP address (determined by the customer's network administrator) in the *IP Address* field.
5. Type the switch subnet mask (determined by the customer's network administrator) in the *Subnet Mask* field.
6. At the *Data Source for Domain* area of the dialog box, select the *Use auto detection*, *Use the server*, or *Use a specific RDC* radio button (determined by the customer's network administrator).
7. Click **OK** to save the entered information, close the dialog box, and define the switch to the SAN management application.
8. Repeat [step 2](#) through [step 7](#) for each new switch.
9. Click **OK** to close the *Discover Setup* dialog box and return to the SAN management application.

Task 14: Record or Verify Server Restore Information

Windows 2000 operating system configuration information must be recorded to restore the management server in case of hard drive failure. Refer to [Appendix C, *Restore Management Server*](#) for instructions. Record or verify the following management server configuration information:

1. Verify network configuration information is recorded. The information was recorded while performing [Task 7: *Configure Server Password and Network Addresses*](#) on page 2-51 and [Task 8: *Configure Management Server Information*](#) on page 2-55.
 - a. Verify the default LCD panel password (9999) or changed password is recorded.
 - b. Verify default or changed network addresses are recorded for the private LAN connection (LAN 2):
 - **IP address** - default is 10.1.1.1.
 - **Subnet mask** - default is 255.0.0.0.
 - **Gateway address** - default is blank.
 - **DNS server IP address** - default is blank.
 - c. Verify default or changed network addresses are recorded for the public LAN connection (LAN 1):
 - **IP address** - default is 192.168.0.1.
 - **Subnet mask** - default is 255.0.0.0.
 - **Gateway address** - default is blank.
 - **DNS server IP address** - default is blank.
 - d. Verify the default computer name (MGMTSERVER) or changed computer name is recorded.
2. Verify user passwords and other information are recorded. The information was recorded while performing [Task 9: *Configure Windows 2000 Users*](#) on page 2-63.
3. Verify date and time information is recorded. The information was recorded while performing [Task 10: *Set Management Server Date and Time*](#) on page 2-69.

- a. Verify the time zone is recorded.
 - b. Verify if the management server is set to automatically adjust the clock for daylight savings time changes.
4. Record the Product ID number as follows:
- a. At the Windows 2000 desktop, click *Start* at the left side of the task bar, then select *Settings*, then *Control Panel*. The *Control Panel* window displays (Figure 2-50 on page 2-58).
 - b. Double-click the *System* icon. The *System Properties* dialog box displays with the *General* page open (Figure 2-73). Record the Product ID number listed under the *Registered to* heading.

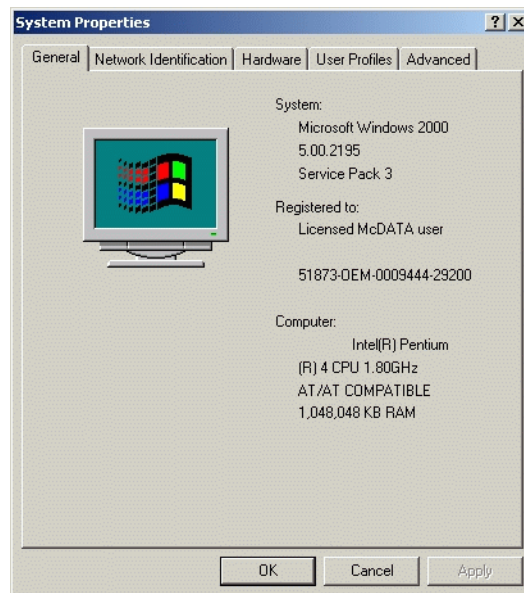


Figure 2-73 System Properties Dialog Box (General Tab)




- c. Click *Cancel* to close the *System Properties* dialog box.
- d. Click close (X) at the upper right corner of the *Control Panel* window to return to the Windows 2000 desktop.

Task 15: Verify Switch-to-Server Communication

Communication must be verified between the switch and server (SAN management and Element Manager applications). To verify switch-to-server communication:

1. At the SAN management application's main window (physical map or product list), inspect the shape and color of the status symbol associated with the Sphereon 4500 Switch product icon. [Table 2-4](#) explains operational states and associated symbols.

Table 2-4 Switch Operational States and Symbols

Operational State	Status Symbol
Operational - switch-to-server communication is established, the switch is operational, and no failures are indicated. Go to Task 16: Configure PFE Key (Optional) on page 2-82.	No status symbol
Degraded - switch-to-server communication is established, but the switch is operating in degraded mode and requires service. This condition is typical if a port or redundant FRU fails. Go to step 2 .	
Failed - switch-to-server communication is established, but the switch failed and requires immediate service. Go to step 2 .	
Status Unknown - the switch status is unknown because of a network communication failure between the switch and management server. Go to step 2 .	

2. Right-click the Sphereon 4500 product icon ([Figure 2-74](#)) at the SAN management application's physical map. A pop-up menu appears.



Figure 2-74 Sphereon 4500 Product Icon

3. Select the *Element Manager* option from the pop-up menu. When the Element Manager application opens, the last view (tab) accessed by a user opens by default. As an example, the *Hardware View* (Figure 2-75) is shown.

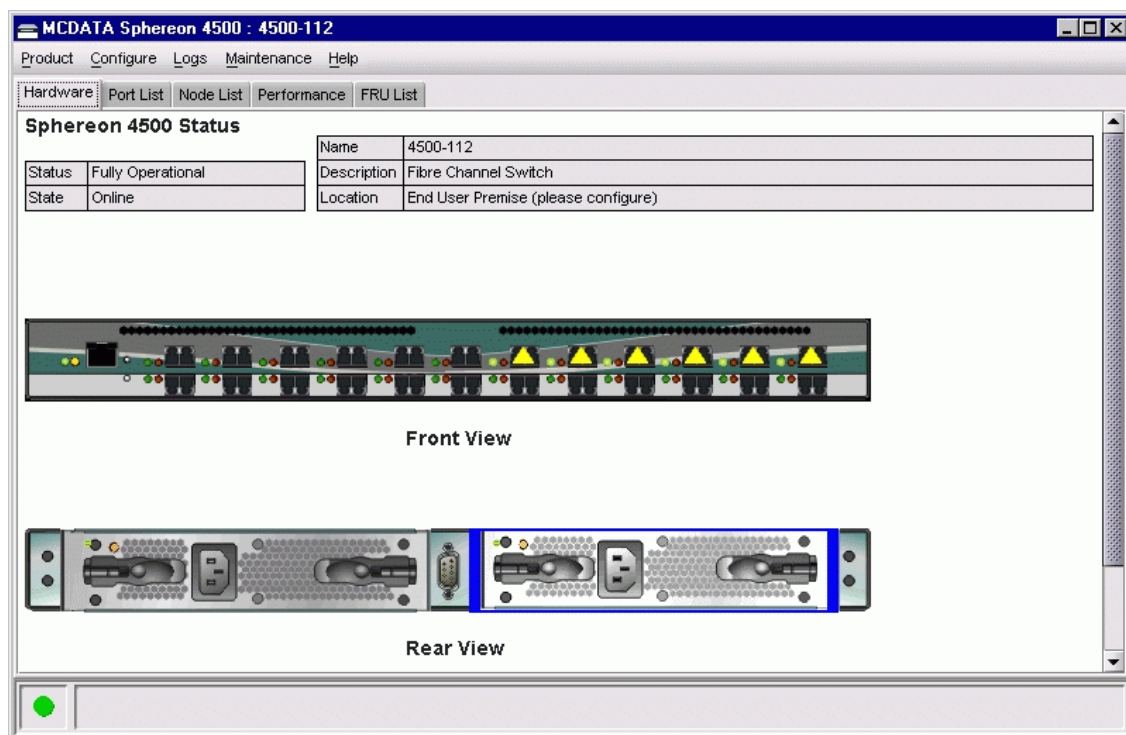


Figure 2-75 Hardware View

4. Inspect switch status at the *Hardware* view and perform one of the following steps:
 - If the switch appears operational (no FRU alert symbols and a green circle at the status bar), go to [Task 16: Configure PFE Key \(Optional\)](#) on page 2-82.
 - If switch operation appears degraded or a switch failure is indicated (FRU alert symbols and a yellow triangle or red diamond on the status bar), go to [MAP 0000: Start MAP](#) on page 3-6 to isolate the problem.

Task 16: Configure PFE Key (Optional)

Perform this task to display or install operating features that are available for the switch as customer-specified options. Available features include the:

- **OSMS** - These feature allows open systems host control of the switch.
- **Flexport Technology** - A Flexport Technology switch is delivered at a discount with only eight ports enabled. When additional port capacity is required, the remaining ports are enabled (in eight-port increments) through purchase of this feature.
- **SANtegrity binding** - This feature enhances security in SANs with a large and mixed group of fabrics and attached devices.
- **OpenTrunking** - This feature provides dynamic load balancing of Fibre Channel traffic across multiple ISLs.
- **Full volatility** - This feature ensures that no Fibre Channel frames are stored after the switch is powered off, and a memory dump file (that possibly includes classified frames) is not included as part of the data collection procedure.
- **CNT WAN support** - This feature is included *only* in software maintenance release 4.02.00, and is required to allow the switch to communicate with CNT UltraEdge WAN Gateways.
- **Element Manager application** - This feature enables switch management through the Element Manager user interface. The switch is delivered with the application enabled for a 31-day grace period. Before grace period expiration, the application must be reactivated through a PFE key.

During the 31-day grace period, a *No Feature Key* dialog box ([Figure 2-76](#) on page 2-83) appears when the Element Manager application is accessed. Click *OK* to close the dialog box and open the application.

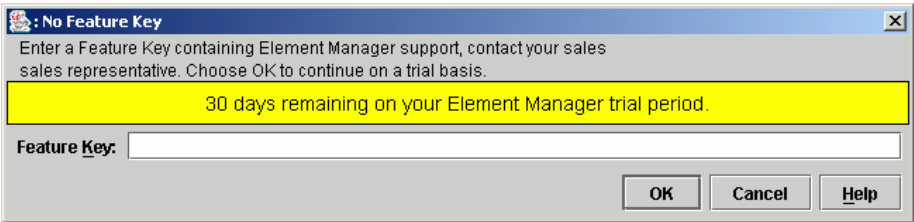


Figure 2-76 No Feature Key Dialog Box

In addition, the message **Element Manager license key has not been installed - Please follow up instructions to update permanent key** appears splashed across views, indicating the Element Manager PFE key must be installed. The *Hardware View* (Figure 2-77) is shown as an example.

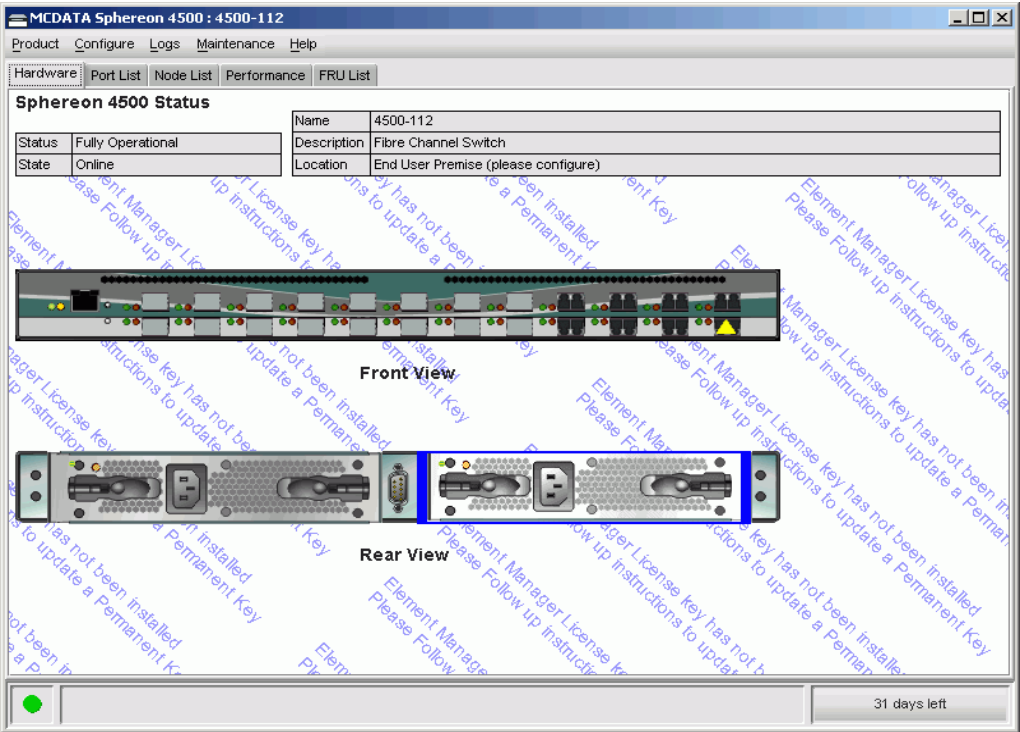


Figure 2-77 Hardware View (with Element Manager Message)

Features are enabled through a PFE key that is encoded to work with the serial number of a unique switch. A key is a case-sensitive alphanumeric string with dashes every four characters. To configure the PFE key:

1. Ensure the switch is set offline. For instructions, refer to [Set the Switch Online or Offline](#) on page 4-48.
2. At the *Hardware View*, click *Configure* at top of the view and select *Features* from the pop-up menu. The *Configure Feature Key* dialog box displays ([Figure 2-78](#)).

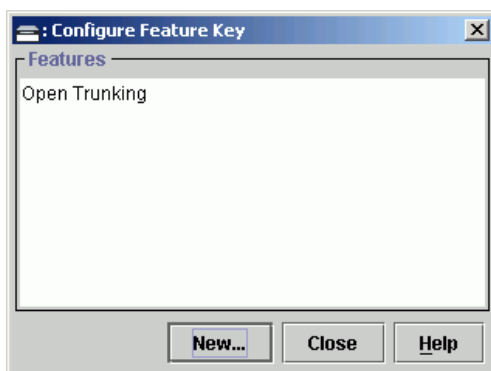


Figure 2-78 Configure Feature Key Dialog Box

3. Click *New*. The *New Feature Key* dialog box displays ([Figure 2-79](#)).



Figure 2-79 New Feature Key Dialog Box

4. Type the PFE key (case-sensitive xxxx-xxxx-xxxx-xx format) and click OK. The *Enable Feature Key* dialog box displays ([Figure 2-80](#) on page 2-85).

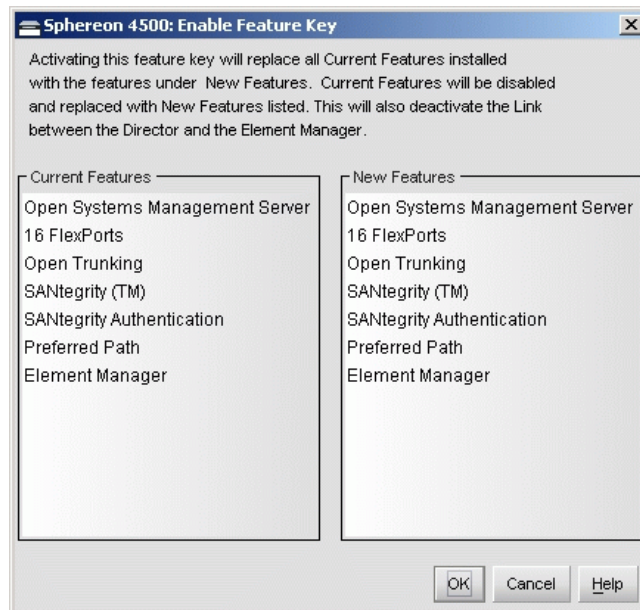


Figure 2-80 Enable Feature Key Dialog Box

- Click *OK*. If the switch is online, it performs an IPL when the PFE key is enabled and a *Warning* dialog box displays (Figure 2-81).

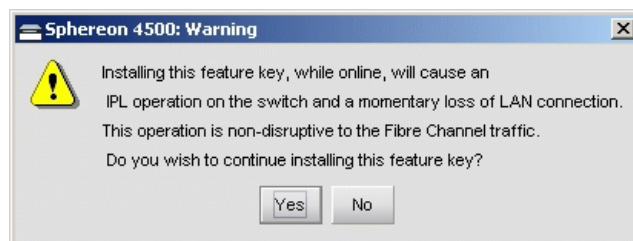


Figure 2-81 Warning Dialog Box

- Click *Yes* to enable the PFE key. When the key is enabled, the switch performs an IPL.
- At the *Configure Feature Key* dialog box, click *Close* to close the dialog box.

NOTE: PFE keys are encoded to work with the serial number of the installed switch only. Record the key to re-install the feature if required. If the switch fails and must be replaced, obtain new PFE keys from the McDATA Solution Center (800-752-4572 or support@mcdata.com). Please have the serial numbers of the failed and replacement switches, and the old PFE key number or transaction code.

Task 17: Configure Management Server (Optional)



Perform this procedure to configure the open systems management server and enable OSI host control of the switch. Implementing host control requires installation of a SAN management application on the OSI server. Management applications include Veritas® SANPoint™ Control (version 1.0 or later), or Tivoli® NetView® (version 6.0 or later). To configure the open systems management server:

1. At the *Hardware View*, click *Configure* at top of the view and select *Open Systems Management Server* from the pop-up menu. Two submenu options display:
 - *Enable OSMS*.
 - *Host Control Prohibited*.
2. Enable or disable the open systems management server by selecting the *Enable OSMS* option. Check the box to enable the server. An unchecked box indicates the server is disabled.
3. Allow or prohibit host (OSI server) control by selecting the *Host Control Prohibited* option. Check the box to prohibit a host management program from changing configuration and connectivity parameters on the switch. The host program has read-only access to configuration and connectivity parameters. An unchecked box allows a host management program to change configuration and connectivity parameters.

Task 18: Set Switch Date and Time

Sphereon 4500 Element Manager log entries are stamped with the date and time received from the switch. To set the effective date and time for the switch:

1. At the *Hardware View*, select *Date/Time* from the *Configure* menu. The *Configure Date and Time* dialog box displays (Figure 2-82).

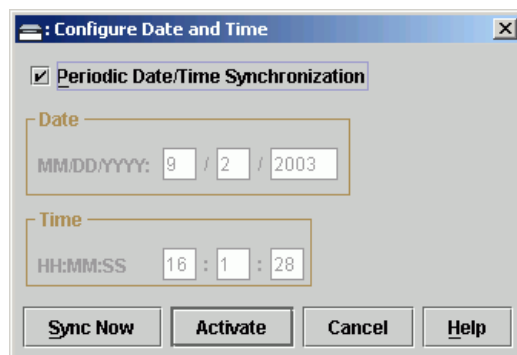


Figure 2-82 Configure Date and Time Dialog Box

The switch date and time can be set manually, or set to be periodically updated by the SAN management application (the switch and application synchronize at least once daily).

2. To set the switch date and time manually:
 - a. Click the *Periodic Date/Time Synchronization* check box to deselect the option (no check mark in the box). The greyed out *Date* and *Time* fields activate.
 - b. Click the *Date* fields that require change, and type numbers in the following ranges:
 - Month (MM): 1 through 12.
 - Day (DD): 1 through 31.
 - Year (YYYY): greater than 1980.
 - c. Click the *Time* fields that require change, and type numbers in the following ranges:
 - Hour (HH): 0 through 23.
 - Minute (MM): 0 through 59.
 - Second (SS): 0 through 59.
 - d. Click *Activate* to set the switch date and time and close the *Configure Date and Time* dialog box.

3. To set the switch to periodically synchronize date and time with the SAN management application:
 - a. Click the *Periodic Date/Time Synchronization* check box to select the option (check mark in the box). The *Date* and *Time* fields are greyed out and not selectable. Perform one of the following options:
 - Click *Activate* to enable synchronization and close the *Configure Date and Time* dialog box. The switch date and time synchronize with the SAN management application date and time at the next update period (at least once daily).
 - Click *Sync Now* to synchronize the switch and SAN management application immediately. The *Date and Time Synced* information dialog box displays (Figure 2-83).

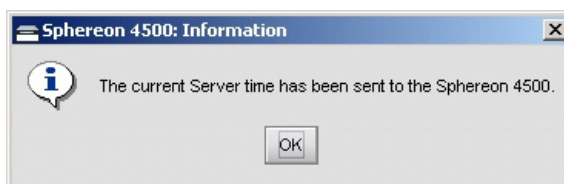


Figure 2-83 Date and Time Synced Dialog Box

- b. Click *OK* to synchronize the date and time and close the *Date and Time Synced* dialog box, then click *Activate* to enable synchronization and close the *Configure Date and Time* dialog box.

Task 19: Configure the Sphereon 4500 Element Manager Application

Selectively perform one or more of the following configuration tasks for the Sphereon 4500 Element Manager application according to the customer's installation requirements:

- Identify the switch to the SAN management (SANavigator 4.0 or EFCM 8.0) application (configure switch identification).
- Configure switch and fabric operating parameters.

- Configure preferred paths.
- Configure switch binding.
- Configure switch ports.
- Configure SNMP trap message recipients.
- Configure threshold alerts.
- Configure OpenTrunking.
- Enable SANpilot interface and Telnet access.
- Configure and enable e-mail notification.
- Configure and enable Ethernet events.
- Configure and enable call-home event notification.

Configure Switch Identification

Perform this procedure to configure the switch name, description, location, and contact person for the SAN management application. The information appears in multiple dialog boxes throughout the application. In addition, the *Name*, *Location*, and *Contact* variables configured at the *Configure Identification* dialog box correspond respectively to the SNMP variables *sysName*, *sysLocation*, and *sysContact*. These variables are used by SNMP management workstations when obtaining data from managed switches.

To configure the switch identification:

1. At the *Hardware View*, select *Identification* from the *Configure* menu. The *Configure Identification* dialog box displays (Figure 2-84).

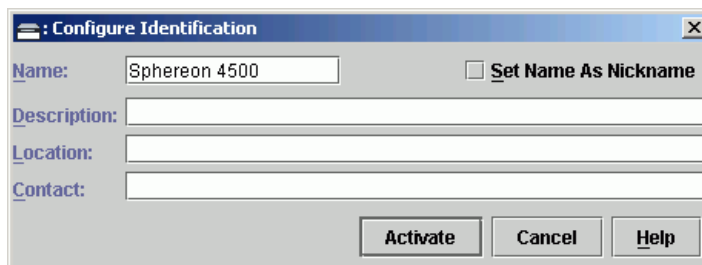


Figure 2-84 Configure Identification Dialog Box

- a. Type a switch name of 24 alphanumeric characters or less in the *Name* field. Each switch should be configured with a unique name.

If the switch is installed on a public LAN, the name should reflect the switch's Ethernet network DNS host name. For example, if the DNS host name is **sphereon4500.mcdata.com**, the name entered in this dialog box should be **Sphereon 4500**.

- b. Type a switch description of 255 alphanumeric characters or less in the *Description* field.
- c. Type the switch's physical location (255 alphanumeric characters or less) in the *Location* field.
- d. Type the name of a contact person (255 alphanumeric characters or less) in the *Contact* field.
- e. Click *Set Name as Nickname* to add a check mark to the check box if you want to use the name in the *Name* field as a nickname for the switch's WWN. The nickname will then display instead of the WWN in Element Manager application Views.

2. Click *Activate* to save the information and close the dialog box.

Configure Switch Parameters

Perform this procedure to configure the switch's preferred domain ID, insistent domain ID, rerouting delay, and domain RSCNs. The switch must be set offline to configure the preferred domain ID. To configure switch parameters:

1. Ensure the switch is set offline. For instructions, refer to [Set the Switch Online or Offline](#) on page 4-48.
2. At the *Hardware View*, select *Operating Parameters*, then *Switch Parameters* from the *Configure* menu. The *Configure Switch Parameters* dialog box displays ([Figure 2-85](#) on page 2-91).

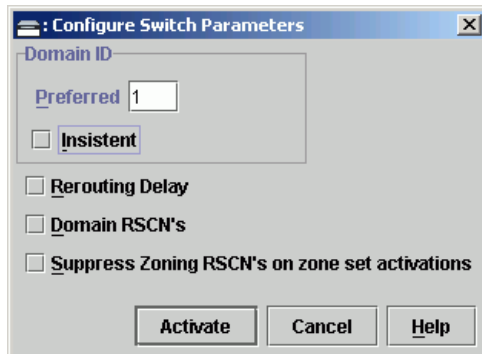


Figure 2-85 Configure Switch Parameters Dialog Box

- a. At the *Preferred Domain ID* field, type a value between 1 through 31. The domain ID uniquely identifies each switch in a fabric.

NOTE: If the switch is attached to a fabric element, the switch and element must have unique domain IDs. If the values are not unique, the E_Port connection to the element segments and the switch cannot communicate with the fabric.

- b. Click the *Insistent Domain ID* check box to enable or disable this parameter. A check mark in the box indicates the parameter is enabled. When the parameter is enabled, the domain ID configured in the *Preferred Domain ID* field becomes the active domain identification when the fabric initializes.
- c. Click the *Rerouting Delay* check box to enable or disable this parameter. A check mark in the box indicates the parameter is enabled. When the parameter is enabled, traffic is delayed through the fabric by the specified E_D_TOV. This delay ensures Fibre Channel frames are delivered to their destination in order, even if a change to the fabric topology creates a new (shorter) transmission path.
- d. Click the *Domain RSCN's* check box to enable or disable this parameter. A check mark in the box indicates the parameter is enabled. When the parameter is enabled, attached devices can register to receive notification when another attached device changes state.

- e. Click the *Suppress RSCNs on zone set activations* check box to enable or disable this parameter. A check mark in the box indicates the parameter is enabled, and is the default. When the parameter is enabled (checked), attached devices do not receive notification following any change to the fabric's active zone set. When the parameter is disabled, attached devices (registered through the fabric format domain register) do receive notification following any change to the fabric's active zone set.
3. Click *Activate* to save the information and close the dialog box.
4. Set the switch online. For instructions, refer to [Set the Switch Online or Offline](#) on page 4-48.

Configure Fabric Parameters

Perform this procedure to configure the fabric operating parameters, including R_A_TOV, E_D_TOV, switch priority, and interop mode. The switch must be set offline. To configure fabric parameters:

1. Ensure the switch is set offline. For instructions, refer to [Set the Switch Online or Offline](#) on page 4-48.
2. At the *Hardware View*, select *Operating Parameters*, then *Fabric Parameters* from the *Configure* menu. The *Configure Fabric Parameters* dialog box displays ([Figure 2-86](#)).

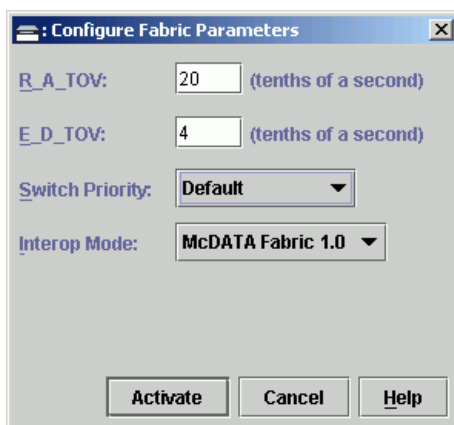


Figure 2-86 Configure Fabric Parameters Dialog Box

- a. At the R_A_TOV field, type a value between **10** through **1200** tenths of a second (one through 120 seconds).

NOTE: If the switch is attached to a fabric element, the switch and element must be set to the same R_A_TOV value. If the values are not identical, the E_Port connection to the element segments and the switch cannot communicate with the fabric. In addition, the R_A_TOV value must be greater than the E_D_TOV value.

- b. At the *E_D_TOV* field, type a value between **2** through **600** tenths of a second (0.2 through 60 seconds).

NOTE: If the switch is attached to a fabric element, the switch and element must be set to the same E_D_TOV value. If the values are not identical, the E_Port connection to the element segments and the switch cannot communicate with the fabric. In addition, the E_D_TOV value must be less than the R_A_TOV value.

- c. Select from the *Switch Priority* drop-down list to set the switch priority. Available selections are *Default*, *Principal*, and *Never Principal*. The default setting is *Default*.

This value designates the fabric's principal switch. The principal switch is assigned a priority of **1** and controls the allocation and distribution of domain IDs for all fabric elements (including itself).

Principal is the highest priority setting, *Default* is the next highest, and *Never Principal* is the lowest priority setting. The setting *Never Principal* means the switch is incapable of becoming a principal switch. If all switches are set to *Principal* or *Default*, the switch with the highest priority and the lowest WWN becomes the principal switch.

At least one switch in a fabric must be set as *Principal* or *Default*. If all switches are set to *Never Principal*, all ISLs segment.

- d. Select from the *Interop Mode* drop-down list to set the switch operating mode. This setting only affects the mode used to manage the switch; it does not affect port operation. Available selections are:
- **McDATA Fabric 1.0** - Select this option if the switch is fabric-attached only to other McDATA directors or switches operating in McDATA fabric mode.

- **Open Fabric 1.0** - Select this option (default) for managing heterogeneous fabrics and if the switch is fabric-attached to McDATA directors or switches and open-fabric compliant switches produced by other OEMs.
3. Click *Activate* to save the information and close the dialog box.
 4. Set the switch online. For instructions, refer to [Set the Switch Online or Offline](#) on page 4-48.

Configure Preferred Paths

The preferred path option allows a user to specify and configure one or more ISL data paths between multiple directors or switches in a fabric. Each participating director or switch must be configured as part of a desired path. The following rules apply when configuring a preferred path:

- The switch domain ID must be set to *Insistent*. For instructions, refer to [Configure Switch Parameters](#) on page 2-90.
- Domain IDs range between **1** through **31**.
- Source and exit port numbers are limited to the range of ports available on the director or switch (**0** through **23**).
- For each source port, only one path is defined to each destination domain ID.

ATTENTION ! Activating a preferred path can result in receipt of out-of-order frames if the preferred path differs from the current path, if input and output (I/O) is active from the source port, and if congestions is present on the current path.

To configure one or more preferred paths for the switch:

1. At the *Hardware View*, select *Preferred Path* from the *Configure* menu. The *Configure Preferred Paths* dialog box displays ([Figure 2-87](#) on page 2-95).

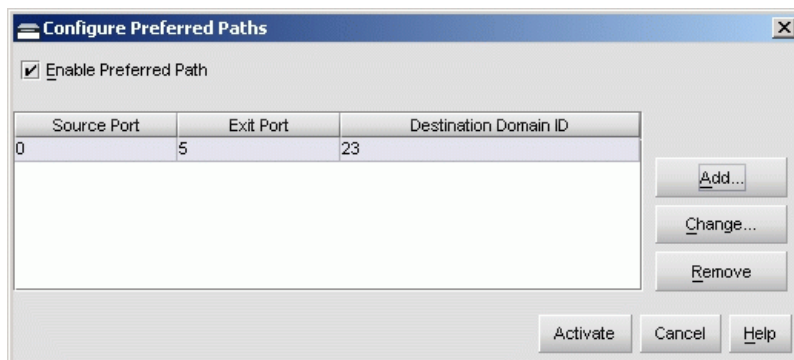


Figure 2-87 Configure Preferred Paths Dialog Box

- Click *Add*. The *Add Preferred Path* dialog box displays (Figure 2-88).

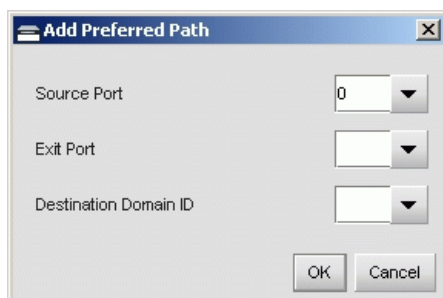


Figure 2-88 Add Preferred Path Dialog Box

- At the *Source Port* field, type a value between 0 through 23. For this switch, the value uniquely identifies the starting port for the preferred path.
- At the *Exit Port* field, type a value between 0 through 23. For this switch, the value uniquely identifies the exit port for the preferred path.
- At the *Destination Domain ID* field, type a value between 1 through 31. This value uniquely identifies the destination director or switch in the path.
- Click *OK* to close the *Add Preferred Path* dialog box and add the path to the list at the *Configure Preferred Paths* dialog box.

7. Repeat [step 2](#) through [step 6](#) to configure additional preferred paths.
8. At the *Configure Preferred Paths* dialog box, select (click) the *Enable Preferred Path* check box.
9. Click *Activate* to enable all configured preferred paths and close the dialog box.

Configure Switch Binding

The switch binding (SANtegrity binding) feature specifies devices that can connect to Sphereon 4500 switch ports. This provides security in SAN environments by ensuring that only an intended set of devices can communicate with the switch.

Overview

To configure switch binding, enable the feature and select the type of port for which connection is to be restricted (connection policy). Port selections include *E_Ports*, *F_Ports*, or all port types. For instructions, refer to [Enable or Disable Switch Binding](#) on page 2-97.

If the switch is online, binding populates a membership list at the *Switch Binding - Membership List* dialog box displays ([Figure 2-90](#) on page 2-99) with WWNs of devices connected to the switch. The list is modified by the connection policy set in the *Switch Binding - Change State* dialog box displays ([Figure 2-89](#) on page 2-98). When the switch binding feature is first installed but not enabled, the associated membership list is empty. The list is populated with device WWNs as follows:

- When switch binding is enabled with the switch online, the membership list is automatically populated with the WWNs of all devices and fabric elements connected to the switch.
- When switch binding is enabled with the switch offline, the membership list is not automatically populated.
- After enabling switch binding, prohibit devices from connecting with switch ports by removing the devices from the membership list. Allow devices to connect to switch ports by adding the devices to the membership list.

Online State and Switch Binding

Specific operating parameters and optional features must be enabled for switch binding to function. In addition, there are requirements for disabling these parameters and features when the switch is online or offline. Be aware that:

- Switch binding can be enabled or disabled when the switch is either offline or online.
- If Enterprise Fabric Mode is enabled from the SAN management application:
 - Switch binding is automatically enabled.
 - Switch binding cannot be disabled if the switch is online.
 - Switch binding can be disabled if the switch is offline. However, if switch binding is disabled, Enterprise Fabric Mode is also disabled.
- WWNs can be added to the membership list when switch binding is either enabled or disabled.
- WWNs can be removed from the membership list **only** if one or more of the following are true:
 - The switch is offline.
 - Switch binding is disabled.
 - The associated device is not connected to the switch.
 - The associated device is connected to a blocked port.
 - Switch binding is not enabled for the same port type as enabled at the *Switch Binding - Change State* dialog box (Connection Policy). For example, a WWN for a fabric switch connected to an E_Port can be removed if switch binding is enabled to restrict only F_Ports.
- If the switch is online and switch binding is not enabled, all WWNs of devices attached to the switch are automatically added to the membership list.

Zoning and Switch Binding

SANtegrity binding parameters have no effect on zoning configurations. However, if a device WWN is in a specific zone, but the WWN is not in the membership list, the device cannot log in to a switch port and cannot connect to other devices in the zone with switch binding enabled.

Enable or Disable Switch Binding

Perform this procedure to configure (enable or disable) switch binding:

1. Ensure the SANtegrity binding PFE key is installed and configured. For instructions, refer to [Task 16: Configure PFE Key \(Optional\)](#) on page 2-82.
2. At the *Hardware View*, select *Switch Binding*, then *Change State* from the *Configure* menu. The *Switch Binding - State Change* dialog box displays ([Figure 2-89](#)).

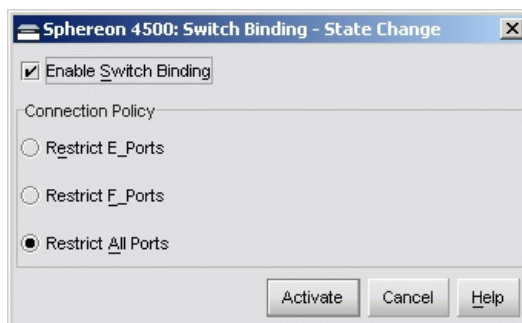


Figure 2-89 Switch Binding - State Change Dialog Box

3. Perform one of the following:
 - To enable switch binding, click the *Enable Switch Binding* check box to add a check mark. Go to [step 4](#) to set the connection policy.
 - To disable switch binding, click the *Enable Switch Binding* check box to remove the check mark, then click *Activate* to enable the change and close the dialog box.
4. Select a *Connection Policy* radio button as follows:
 - **Restrict E_Ports** - Select this button to restrict connections from specific fabric elements to switch E_Ports. WWNs can be added to the membership list to allow element connection and removed from the list to prohibit element connection. Devices are allowed to connect to any F_Port or FL_Port without restriction.
 - **Restrict F_Ports** - Select this button to restrict connections from specific devices to switch F_Ports or FL_Ports. WWNs can be added to the membership list to allow device connection and removed from the list to prohibit device connection. Fabric switches are allowed to connect to any E_Port without restriction.

- **Restrict All Ports** - Select this button to restrict connections from specific devices to switch F_Ports or FL_Ports and fabric elements to switch E_Ports. WWNs can be added to the membership list to allow connection and removed from the list to prohibit connection.
5. Click *Activate* to enable the changes and close the *Switch Binding - Change State* dialog box.

Edit Membership List

Perform this procedure to edit the switch binding membership list:

1. Ensure the SANtegrity binding PFE key is installed and configured. For instructions, refer to [Task 16: Configure PFE Key \(Optional\)](#) on page 2-82.
2. At the *Hardware View*, select *Switch Binding*, then *Edit Membership List* from the *Configure* menu. The *Switch Binding - Membership List* dialog box displays (Figure 2-90). WWNs of devices that are allowed to connect to switch ports appear in the *Switch Membership List* panel.

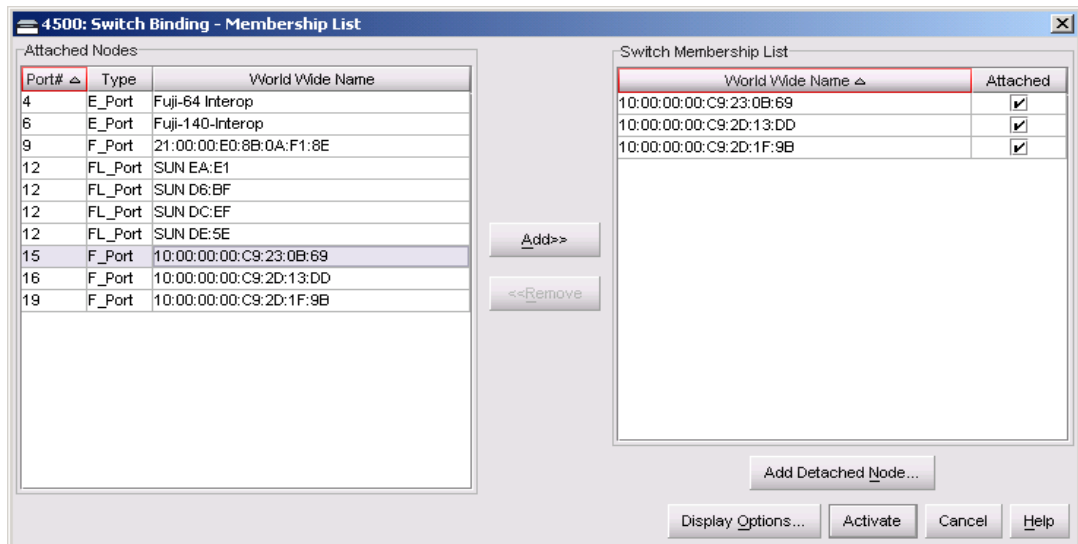


Figure 2-90 Switch Binding - Membership List Dialog Box

3. If nicknames are configured (through the SAN management application) and are to be displayed instead of WWNs, click *Display Options*. The *Display Options* dialog box displays (Figure 2-91). If nicknames are not configured, go to [step 5](#).

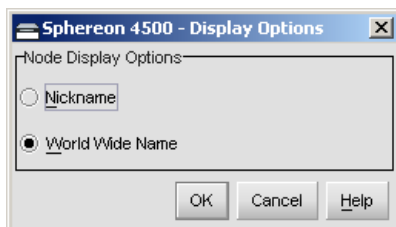


Figure 2-91 Display Options Dialog Box

4. Click the *Nickname* radio button, then click *OK*. The dialog box closes and nicknames appear in the *Switch Binding - Membership List* dialog box.
5. Perform one of the following:
 - To allow a switch port connection to a device listed in the *Node List* Panel, select the WWN or nickname and click *Add>>*. The device WWN or nickname moves to the *Switch Membership List* panel.
 - To prohibit a switch port connection to a device listed in the *Switch Membership List* Panel, select the WWN or nickname and click *<<Remove*. The device WWN or nickname moves to the *Node List* panel.

NOTE: Device connectivity and membership list edits are subject to the rules defined under [Online State and Switch Binding](#) on page 2-96.

6. To add a WWN or nickname for a device not connected to the switch, click *Detached Node*. The *Add Detached Node* dialog box displays (Figure 2-92 on page 2-101).

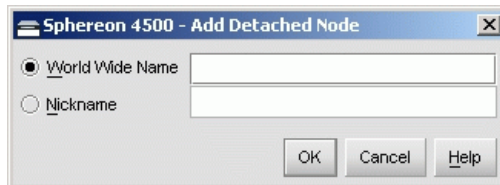


Figure 2-92 Add Detached Node Dialog Box

7. Type the device WWN or nickname and click OK. The WWN or nickname appears in the *Switch Membership List*.
8. Click *Activate* to enable the changes and close the *Switch Binding - Membership List* dialog box.

Configure Switch Ports

To configure switch Fibre Channel ports:

1. At the *Hardware View*, select *Ports* from the *Configure* menu. The *Configure Ports* dialog box displays (Figure 2-93).

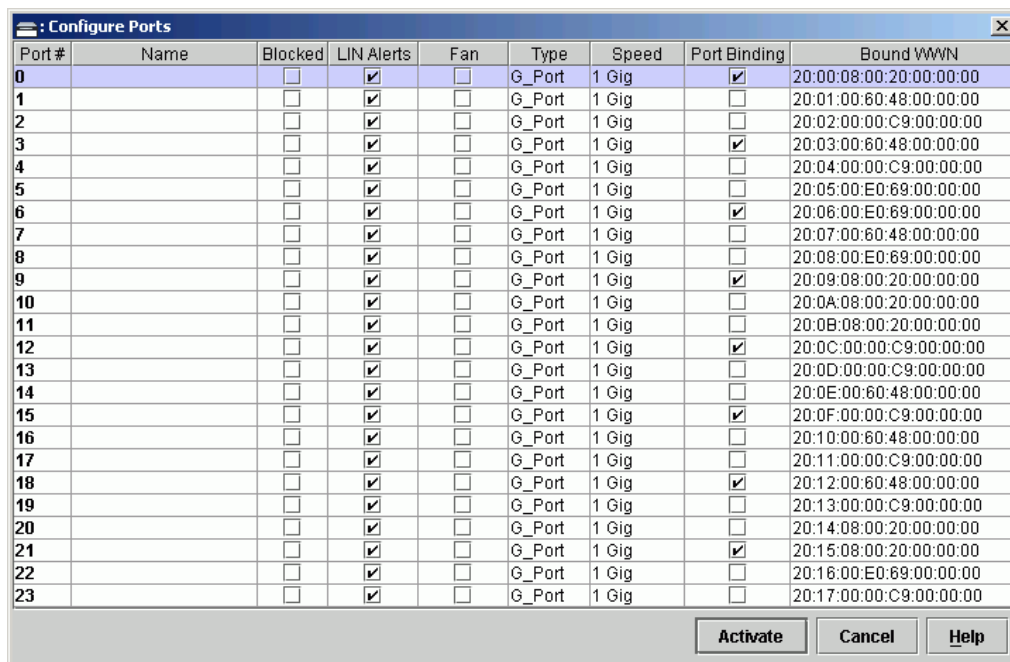


Figure 2-93 Configure Ports Dialog Box

- a. For each port to be configured, type a port name of 24 alphanumeric characters or less in the associated *Name* field. The port name should characterize the device to which the port is attached.
- b. Click a check box in the *Blocked* column to block or unblock a port (default is unblocked). A check mark in the box indicates a port is blocked. Blocking a port prevents the attached devices or fabric switch from communicating. A blocked port continuously transmits the offline sequence (OLS).
- c. Click the check box in the *LIN Alerts* column to enable or disable link incident (LIN) alerts (default is enabled). A check mark in the box indicates alerts are enabled. When the feature is enabled and an incident occurs on the port link, an alert indicator (yellow triangle) displays at the *Hardware View*, and a message is sent to configured e-mail recipients.
- d. Click the check box in the *FAN* column to enable or disable the fabric address notification (FAN) feature (default is enabled). A check mark in the box indicates FAN is enabled. When the feature is enabled, the port transmits a FAN frame after loop initialization to verify that FC-AL devices are still logged in. It is recommended this option be enabled for ports configured for loop operation.
- e. Select from the drop-down list in the *Type* column to configure the port type. Available selections are:
 - Fabric port (**F_Port**).
 - Expansion port (**E_Port**).
 - Generic port (**G_Port**). A generic port setting allows F_Port and E_Port behavior only.
 - Generic mixed port (**GX_Port**). A generic mixed port setting allows F_Port, FL_Port, and E_Port behavior. This is the default selection.
 - Fabric mixed port (**FX_Port**). A fabric mixed port setting allows F_Port and FL_Port behavior only.

2. Select from the drop-down list in the *Speed* column to configure the port transmission rate. Available selections are:
 - Auto-negotiate between 1.0625 and 2.125 Gbps operation (**Negotiate**). This is the default selection.
 - 1.0625 Gbps operation (**1 Gig**).
 - 2.125 Gbps operation(**2 Gig**).
- f. Click the check box in the *Port Binding* column to enable or disable port binding (default is disabled). A check mark in the box indicates port binding is enabled and the port can connect only to a device with a WWN listed in the *Bound WWN* column.
- g. If port binding is enabled, type the WWN or nickname of the device attached to the port in the *Bound WWN* column.
 - If the check box in the *Port Binding* column is checked and a WWN or nickname appears in the *Bound WWN* field, only the specified device can attach to the port.
 - If the check box in the *Port Binding* column is checked but no WWN or nickname appears in the *Bound WWN* field, no device can connect to the port.
 - If the check box in the *Port Binding* column is not checked, any device can connect to the port.
3. Click *Activate* to save the information and close the *Configure Ports* dialog box.

Configure SNMP Trap Message Recipients

Perform this procedure to configure community names, write authorizations, and network addresses and for up to 12 SNMP trap message recipients. A trap recipient is a management workstation that receives notification (through SNMP) if a switch event occurs. To configure SNMP trap recipients:

1. At the *Hardware View*, select *SNMP Agent* from the *Configure* menu. The *Configure SNMP* dialog box displays ([Figure 2-94](#) on page 2-104).

Community Name	Write Authorization	Trap Recipient	UDP Port Number
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		

Buttons: **Activate** **Cancel** **Help**

Figure 2-94 Configure SNMP Dialog Box

- a. For each trap recipient to be configured, type a community name of 32 alphanumeric characters or less in the associated *Community Name* field. The community name is incorporated in SNMP trap messages to ensure against unauthorized viewing or use.
 - b. Click the check box in the *Write Authorization* column to enable or disable write authorization for the trap recipient (default is disabled). A check mark in the box indicates write authorization is enabled. When the feature is enabled, a management workstation user can change the management server's *sysContact*, *sysName*, and *sysLocation* SNMP variables.
 - c. Type the IP address or DNS host name of the trap recipient (SNMP management workstation) in the associated *Trap Recipient* field. Use 64 alphanumeric characters or less. It is recommended the IP address be used.
 - d. The default user datagram protocol (UDP) port number for trap recipients is **162**. To override this default value, type a decimal port number in the associated *UDP Port Number* field.
2. To enable transmission of trap messages to configured SNMP workstations, click the *Enable Authorization Traps* check box. A check mark appears in the box when transmission is enabled.
 3. Click *Activate* to save the information and close the dialog box.

Configure Threshold Alerts

A threshold alert notifies users when an E_Port or F_Port transmit (Tx) or receive (Rx) throughput reaches or exceeds a specified value. Alerts are indicated by:

- An attention indicator (yellow triangle) associated with a port at the *Hardware View*.
- An attention indicator (yellow triangle) in the *Alert* column at the *Port List View*.
- An attention indicator (yellow triangle) in the *Threshold Alerts* field at the *Port Properties* dialog box.
- Data recorded in the *Threshold Alert Log*.

To configure threshold alerts:

1. At the *Hardware View*, select *Threshold Alerts* from the *Configure* menu. The *Configure Threshold Alert(s)* dialog box displays (Figure 2-95).

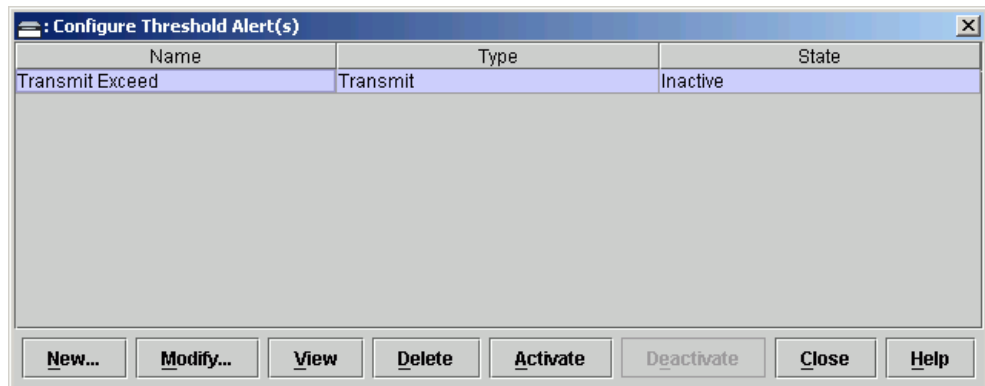


Figure 2-95 Configure Threshold Alert(s) Dialog Box

If alerts are configured, they display in table format showing the alert name, type, and state.

2. Click *New*. The *New Threshold Alert* dialog box (screen 1) displays (Figure 2-96 on page 2-106).

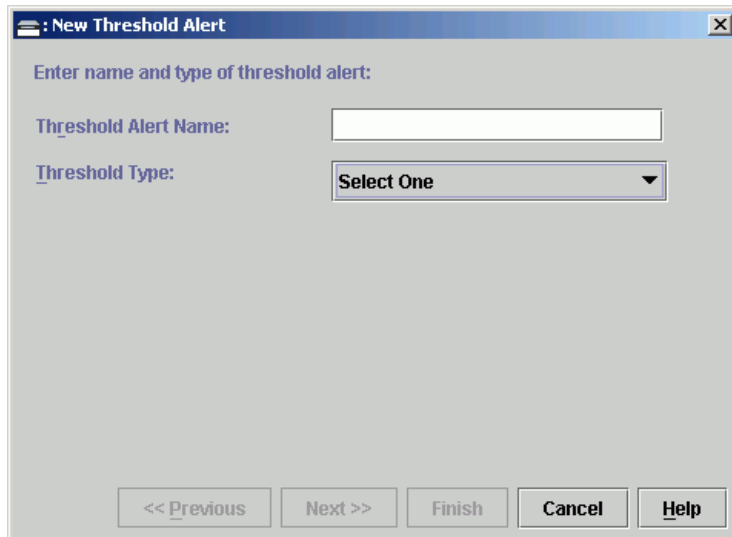


Figure 2-96 New Threshold Alert Dialog Box (Screen 1)

3. Type a name of 64 alphanumeric characters or less in the associated *Threshold Alert Name* field.
4. Select from the *Threshold Alert* drop-down list to configure the alert type. Available selections are:
 - **Rx Throughput** - An alert occurs if the threshold value for receive throughput is reached or exceeded.
 - **Tx Throughput** - An alert occurs if the threshold value for transmit throughput is reached or exceeded.
 - **Rx or Tx Throughput** - An alert occurs if the threshold value for either receive or transmit throughput is reached or exceeded.
5. Click *Next*. The *New Threshold Alert* dialog box (screen 2) displays ([Figure 2-97](#) on page 2-107). The name configured for the alert appears at the top of the dialog box.

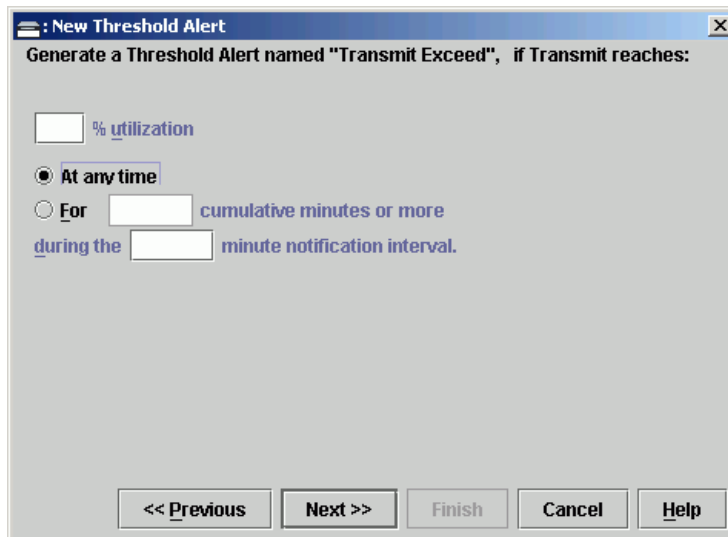


Figure 2-97 New Threshold Alert Dialog Box (Screen 2)

6. Type a percentage from 1 through 100 in the *% utilization* field. When throughput reaches the specified percentage of port capacity, a threshold alert occurs.
7. Enter the cumulative minutes for which the *% utilization* should exist during the notification interval before an alert is generated. Select the *At any time* radio button to specify that an alert occur when the *% utilization* is reached. The valid range is 1 to the interval set in [step 8](#).
8. Enter the interval (in minutes) during which throughput is measured and threshold notifications can occur. The valid range is 5 through 70560 minutes.
9. Click *Next*. The *New Threshold Alert* dialog box (screen 3) displays ([Figure 2-98](#) on page 2-108).

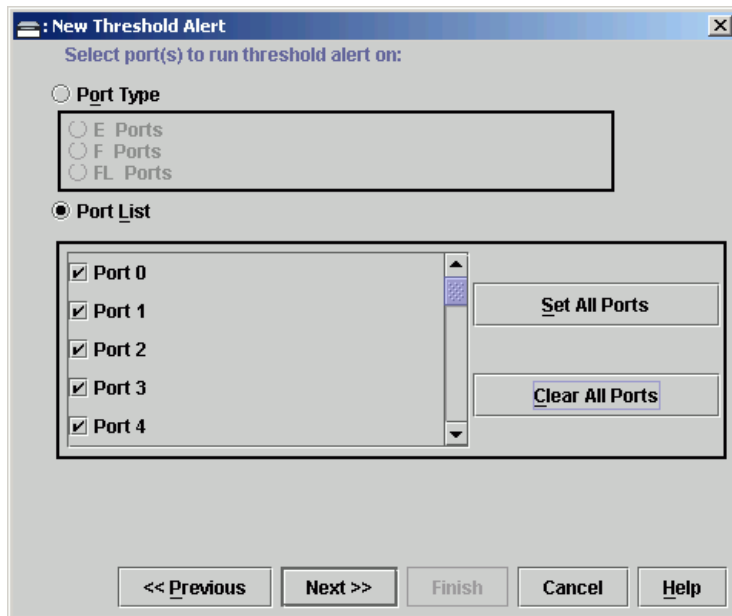


Figure 2-98 New Threshold Alert Dialog Box (Screen 3)

10. Select the *Port Type* or *Port List* radio button.
 - Select *Port Type* radio button, then the *E_Ports*, *F_Ports*, or *FL_Ports* radio button to cause an alert to generate for all ports configured as either *E_Ports*, *F_Ports*, or *FL_Ports*.
 - Select *Port List* to configure individual ports by clicking the check box adjacent to each port number. Select *Set All Ports* to place a check mark adjacent to all port numbers. Select *Clear All Ports* to clear the check marks by port numbers.
11. Click *Next*. The *New Threshold Alert* dialog box (screen4) displays (Figure 2-99 on page 2-109). This screen appears to provide a summary of the alert configuration. To make changes, move back and forth through the configuration screens by selecting *Previous* or *Next*.

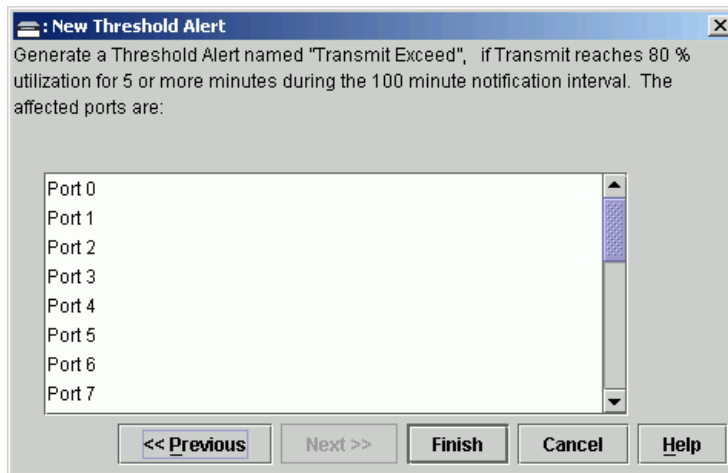


Figure 2-99 New Threshold Alert Dialog Box (Screen 4)

12. Click *Finish*. The *Configure Threshold Alerts* dialog box reappears ([Figure 2-95](#) on page 2-105) listing the name, type, and state of the alert configured.
13. To activate the alert, highlight (select) the alert and click *Activate*.

Configure OpenTrunking

Perform this procedure to configure OpenTrunking parameters. The OpenTrunking feature must be installed to access this control. Refer to [Task 16: Configure PFE Key \(Optional\)](#) on page 2-82 for instructions. To configure OpenTrunking parameters:

1. Ensure the switch is online. For instructions, refer to [Set the Switch Online or Offline](#) on page 4-48.
2. At the *Hardware View*, select *OpenTrunking* from the *Configure* menu. The *Configure OpenTrunking* dialog box displays ([Figure 2-100](#) on page 2-110).

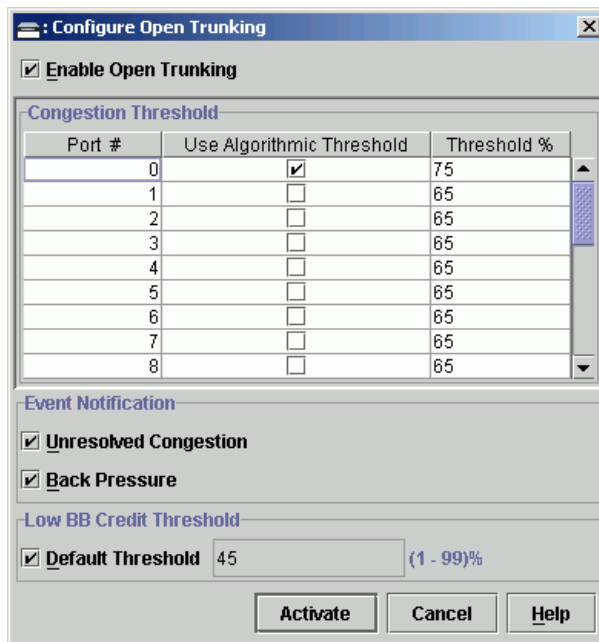


Figure 2-100 Configure OpenTrunking Dialog Box

3. Perform one of the following:
 - To enable OpenTrunking, click the *Enable OpenTrunking* check box to add a check mark. Go to [step 4](#) to set the congestion threshold for each port.
 - To disable OpenTrunking, click the *Enable OpenTrunking* check box to remove the check mark, then click *Activate* to enable the change and close the dialog box.
4. For each switch port:
 - a. Click the check box in the *Use Algorithmic Threshold* column. A check mark appears in the box and a calculated default value appears (1% to 99%) in the associated field in the *Threshold %* column. If the default value is enabled, a value cannot be entered in the *Threshold %* column.
 - b. Ensure the check box in the *Use Algorithmic Threshold* column is blank. At the associated field in the *Threshold %* column, type a percentage value from 1% to 99%.

NOTE: The default congestion threshold is calculated by the switch's firmware.

5. Click the *Unresolved Congestion* check box to add a check mark and enable the parameter. When this parameter is enabled, unresolved congestion events are recorded in the event log, and SNMP trap messages are generated and transmitted (if SNMP is configured).

An unresolved congestion event occurs for a low-BB_Credit ISL when the switch's firmware rerouting algorithm cannot route data flow to an alternate path (because doing so would exceed the alternate path's low BB_Credit threshold).

6. Click the *Backpressure* check box to add a check mark and enable the parameter. When this parameter is enabled, backpressure events are recorded in the event log, and SNMP trap messages are generated and transmitted (if SNMP is configured).

A backpressure event occurs when the percent time an ISL has low BB_Credit exceeds the low BB_Credit threshold.

7. The low BB_Credit threshold is the percent time an ISL is allowed to not transmit data because BB_Credit is unavailable. When the threshold is exceeded, data is rerouted to another ISL. In addition, traffic cannot be rerouted to another low- threshold ISL. Use one of the following to set the low BB_Credit threshold:
 - Click the *Default Threshold* check box. A check mark appears in the box and a calculated default value appears (**1% to 99%**) in the adjacent field. If the default value is enabled, a value cannot be entered in the field.
 - Ensure the *Default Threshold* check box is blank. At the adjacent field, type a percentage value from **1% to 99%**.

NOTE: The default low BB_Credit threshold is calculated by the switch's firmware.

8. Click *Activate* to enable the changes and close the dialog box.

Enable SANpilot Interface and Telnet Access

Perform this procedure to enable SANpilot interface and Telnet access through the maintenance port at the rear of the switch. To enable these functions:

1. To enable the SANpilot interface at the *Hardware View*, select *Enable Web Server* from the *Configure* menu. A check mark appears in the box when the interface is enabled, and the menu closes.
2. To enable Telnet access at the *Hardware View*, select *Enable Telnet* from the *Configure* menu. A check mark appears in the box when access is enabled, and the menu closes.

Configure, Enable, and Test E-mail Notification

Perform this procedure to configure, enable, and test e-mail and simple mail transfer protocol (SMTP) addresses to receive notification of switch (and other product) events. Configure and test procedures are performed at the SAN management application. E-mail notification is enabled for each switch at the Element Manager application. To configure, enable, and test e-mail addresses:

1. Minimize the *Hardware View* (Element Manager application) and return to the SAN management application.
2. At the SANavigator or EFCM main window, select the *Event Notification* and *Email* options from the *Monitor* menu. The *Email Event Notification Setup* dialog box displays ([Figure 2-101](#)).

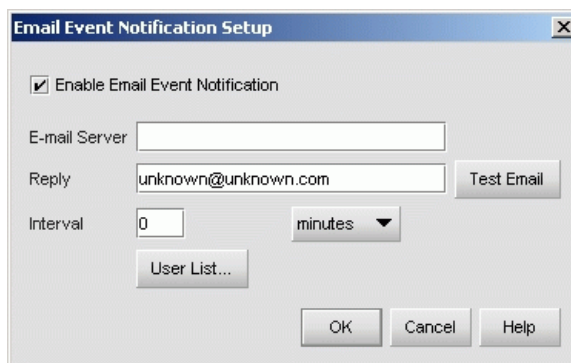


Figure 2-101 Email Event Notification Setup Dialog Box

3. To enable e-mail transmission to configured addresses, click the *Enable Email Event Notification* check box. A check mark appears in the box when transmission is enabled.

NOTE: The enable function must also be activated for each switch through the Sphereon 4500 Element Manager application. E-mail notification can be active for some switches and inactive for others.

4. Type the IP address or DNS host name of the SMTP server in the *E-mail Server* field. It is recommended the IP address be used.
5. Type the e-mail address to which e-mail replies should be sent in the *Reply* field.
6. At the *Interval* field, type the length of time the application should wait between notifications. Choose **seconds**, **minutes**, or **hours** from the associated drop-down list.
7. To specify users that are to receive e-mail notification, click *User List*. The *SANavigator Server Users* or *EFCM 8 Server Users* dialog box displays (Figure 2-69 on page 2-74).
8. To enable e-mail notification for a user, select (click) the check box in the *Email* column. An unchecked box indicates e-mail notification is not enabled.
9. To configure event types for which e-mail notification is sent, select (click) the *Filter* link adjacent to the check box. The *Define Filter* dialog box displays. For instructions on defining event filters, refer to the *SANavigator Software Release 4.0 User Manual* (621-000013) or *EFC Manager Software Release 8.0 User Manual* (620-000170).
10. Click *OK* to close the *SANavigator Server Users* or *EFCM 8 Server Users* dialog box.
11. Click *Test Email*. A test message is sent to configured e-mail recipients.
12. Click *OK* to save the information and close the *Email Event Notification Setup* dialog box.
13. Maximize the *Hardware View* (Element Manager application).
14. At the *Hardware View*, select *Enable E-Mail Notification* from the *Maintenance* menu. A check mark appears in the check box to indicate e-mail notification for the switch is enabled, and the menu closes.

Configure and Enable Ethernet Events

Perform this procedure to configure and enable Ethernet events. An Ethernet event is recorded (after a user-specified time interval) when the switch-to-management server communication link drops. To configure and enable Ethernet events:

1. Minimize the *Hardware View* (Element Manager application) and return to the SAN management application.
2. At the SANavigator or EFCM main window, select the *Ethernet Event* option from the *Monitor* menu. The *Configure Ethernet Events* dialog box displays ([Figure 2-102](#)).

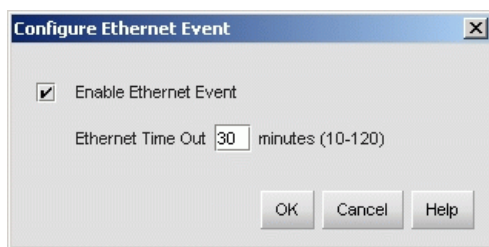


Figure 2-102 Configure Ethernet Events Dialog Box

3. Click the *Enable Ethernet Events* check box. A check mark appears in the check box to indicate Ethernet events are enabled.
4. At the *Ethernet Timeout* field, type a value between **10** through **120** minutes.
5. Click **OK** to close the dialog box.

Configure, Enable, and Test Call-Home Event Notification

Telephone numbers and other information for the call-home feature are configured through the Windows 2000 dial-up networking application. Refer to [Task 11: Configure the Call-Home Feature \(Optional\)](#) for configuration instructions. To configure, enable, and test call-home event notification:

NOTE: The call-home feature may not be available if the EFC Management applications (EFCM Lite) are installed on a customer-supplied platform.

1. Minimize the *Hardware View* (Element Manager application) and return to the SAN management application.

2. At the SANavigator or EFCM main window, select the *Event Notification* and *Call Home* options from the *Monitor* menu. The *Call Home Event Notification Setup* dialog box displays (Figure 2-103).

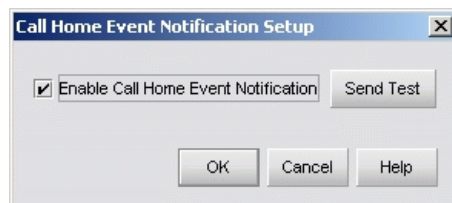


Figure 2-103 Call Home Event Notification Setup Dialog Box

3. Click the *Enable Call Home Event Notification* check box. A check mark appears in the check box to indicate call-home event notification is enabled.

NOTE: The enable function must also be activated for each switch through the Sphereon 4500 Element Manager application. Call-home event notification can be active for some switches and inactive for others.

4. Click *Send Test*. A call-home test message is sent.
5. Click *OK* to close the dialog box.
6. Maximize the *Hardware View* (Element Manager application).
7. At the *Hardware View*, select *Enable Call Home Notification* from the *Maintenance* menu. A check mark appears in the check box to indicate call-home event notification for the switch is enabled, and the menu closes.

Task 20: Back Up Configuration Data

For the Sanavigator 4.0 application, critical configuration data is stored on the management server hard drive in the following directories:

- C:\Program Files\SANavigator4.0\CallHome
- C:\Program Files\SANavigator4.0\Client
- C:\Program Files\SANavigator4.0\Server.

For the EFCM 8.0 application, critical configuration data is stored on the management server hard drive in the following directories:

- **C:\Program Files\EFCM 8.0\CallHome**
- **C:\Program Files\EFCM 8.0\Client**
- **C:\Program Files\EFCM 8.0\Server.**

The server is configured to automatically mirror the contents of these directories to the CD-RW drive anytime directory contents change or the server is rebooted. The directories contain all SAN management configuration data, and are used to restore the management server operating environment in case of hard drive failure. The directories contain:

- SAN management configuration data (switch definitions, user names and passwords, switch date and time, port configurations, operating parameters, SNMP recipients, and e-mail recipients).
- Log files (SAN management application logs and Sphereon 4500 Element Manager application logs).
- Switch firmware versions stored in the firmware library.
- Call-home configuration data.
- Configuration data for the switch is stored in nonvolatile random access memory (NV-RAM) on the switch's CTP card, and is backed up through the Element Manager application. The data is recorded in the directory when a backup is performed.

The server does not back up Windows 2000 operating system data, such as user names, passwords, date and time, and TCP/IP network information. This information was recorded while performing installation tasks, and verified while performing [Task 14: Record or Verify Server Restore Information](#) on page 2-78.

To back up management server configuration data and create a base restore CD:

1. Insert a blank rewritable CD into the CD-RW drive and format the CD:
 - a. At the Windows 2000 desktop, locate the *InCD* icon at the right side of the task bar ([Figure 2-104](#) on page 2-117).



Figure 2-104 InCD Icon (Unformatted CD)

- b. Right-click the icon and select *Format (F)*. The first window of the *InCD* wizard displays (Figure 2-105).

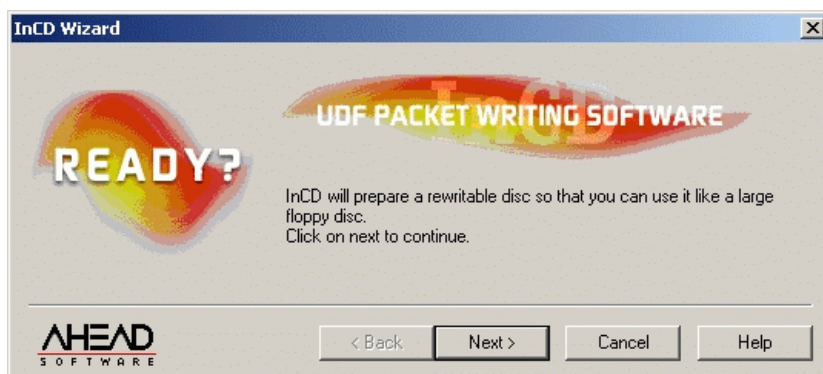


Figure 2-105 InCD Wizard (First Window)

- c. Click *Next* to proceed to the second window of the *InCD* wizard. Use the default parameters displayed at each window, and click *Next* and *Finish* as appropriate to complete the CD formatting task.
- d. When the rewritable CD is formatted, the red down arrow associated with the *InCD* icon changes to a green up arrow (Figure 2-106).

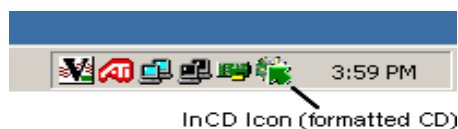


Figure 2-106 InCD Icon (Formatted CD)

2. Back up the switch configuration file to the management server. For instructions, refer to [Back Up the Configuration](#) on page 4-79.

3. If the Hardware View is open, close the view and return to the SAN management application (SANavigator 4.0 or EFCM 8.0) by clicking close (X) at the upper right corner of the window.
4. Close the SAN management application by selecting *Shutdown* from the *SAN* menu. A *SANavigator* or *EFCM Message* dialog box displays (Figure 2-107).

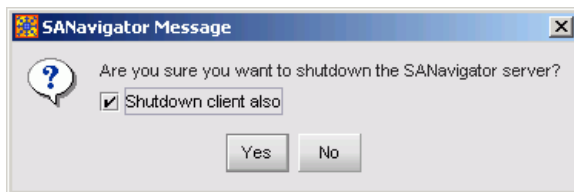


Figure 2-107 SANavigator or EFCM Message Dialog Box

5. Click *Yes* to close the SAN management application.
6. Reboot the management server to cause directory contents to be written to the blank CD:
 - a. At the Windows 2000 desktop, click *Start* at the left side of the task bar (bottom of the desktop), then select *Shut Down*. The *Shut Down Windows* dialog box displays (Figure 2-108).



Figure 2-108 Shut Down Windows Dialog Box

- b. Select the *Restart* option from the list box and click OK. The management server powers down and restarts. During the reboot process the LAN connection between the management server and browser-capable PC drops momentarily, and the TightVNC viewer displays a network error as shown in [Figure 2-109](#) on page 2-119.

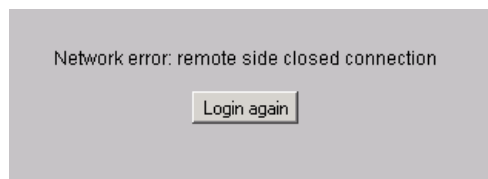


Figure 2-109 TightVNC Network Error Message

- c. After the management server reboots, click *Login again*. The *VNC Authentication* screen displays.
- d. Type the default password and click OK. The *Welcome to Windows* dialog box displays.

NOTE: The default TightVNC viewer password is **password**.

- e. Click the **Send Ctrl-Alt-Del** button at the top of the window to log on to the management server desktop. The *Log On to Windows* dialog box displays ([Figure 2-48](#) on page 2-57).

NOTE: Do not simultaneously press the **Ctrl**, **Alt**, and **Delete** keys. This action logs the user on to the browser-capable PC, not the rack-mount management server.

- f. Type the default Windows 2000 user name and password and click OK. The management server's Windows 2000 desktop opens and the *SANavigator Log In* or *EFCM Log In* dialog box displays ([Figure 2-49](#) on page 2-57).

NOTE: The default Windows 2000 user name is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

- g. Type the SAN management application default user ID and password and select a server or IP address from the *Network Address* drop-down list.

NOTE: The default SAN management application user ID is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

- h. Click *Login*. The application opens and the SANavigator or EFCM main window appears (Figure 2-68 on page 2-73).
7. Remove the base restore CD from the CD-RW drive and store the CD in a safe location. Insert a blank rewritable CD into the CD-RW drive and format the CD. Refer to [step 1](#) for formatting instructions.
8. Go to [Task 21: Cable Fibre Channel Ports](#) below.

Task 21: Cable Fibre Channel Ports

Perform this task to connect devices to the switch. To cable Fibre Channel ports:

1. Route fiber-optic jumper cables from customer-specified Fibre Channel devices, FC-AL devices, or fabric switches to ports at the front of the switch.
2. Connect device cables to SFP optical port transceivers. Start with port 0 (far right) and continue sequentially to the left through port 23.
3. Perform one of the following:
 - If the switch is installed on a table or desk top, bundle and secure the Fibre Channel cables as directed by the customer.
 - If the switch is installed in a customer-supplied equipment rack, bundle Fibre Channel cables from the switch and other equipment (groups of 16 maximum), and secure them as directed by the customer.
 - If the switch is installed in a McDATA Fabriccenter equipment cabinet, bundle Fibre Channel cables from the switch and other equipment (groups of 16 maximum), and secure them in the cable management area at the front-left side of the cabinet.

Task 22: Configure Zoning (Optional)

Perform this procedure to:

- Configure, change, add, or delete zones. A zone is a group of devices that can access each other through port- to-port connections. Devices in the same zone can recognize and communicate with each other; devices in different zones cannot.
- Configure, change, enable, or disable zone sets. A zone set is a group of zones that is activated or deactivated as a single entity across all managed products in either a single switch or a multiswitch fabric. Only one zone set can be active at one time.

If the installation is being performed from the SANpilot interface, go to [Configure Zones \(SANpilot Interface\)](#) below. If the installation is being performed from the management server, zoning is configured on a fabric-wide basis through the SAN management application. Refer to the *SANavigator Software Release 4.0 User Manual* (621-000013) or *EFC Manager Software Release 8.0 User Manual* (620-000170) for instructions.

Configure Zones (SANpilot Interface)

To configure zones at the SANpilot interface:

1. At the *Configure* panel, click the *Zoning* tab. The *Zoning* page displays with the *Zone Set* tab selected. Click the *Zones* tab. The *Zoning* page displays with the *Zones* tab selected ([Figure 2-110](#) on page 2-122).
2. To configure a zone, first add the zone name to the zoning library. The following naming conventions apply to zones and zone sets:
 - All names must be unique and may not differ by case only. For example, **zone-1** and **Zone-1** are both valid individually, but are not considered unique.
 - The first character of a zone set name must be a letter (**A** through **Z** or **a** through **z**).
 - A zone set name cannot contain spaces.
 - Valid characters are alphanumeric and the caret (**^**), hyphen (**-**), underscore (**_**), or dollar (**\$**) symbols.
 - A zone set name can have a maximum of 64 characters.

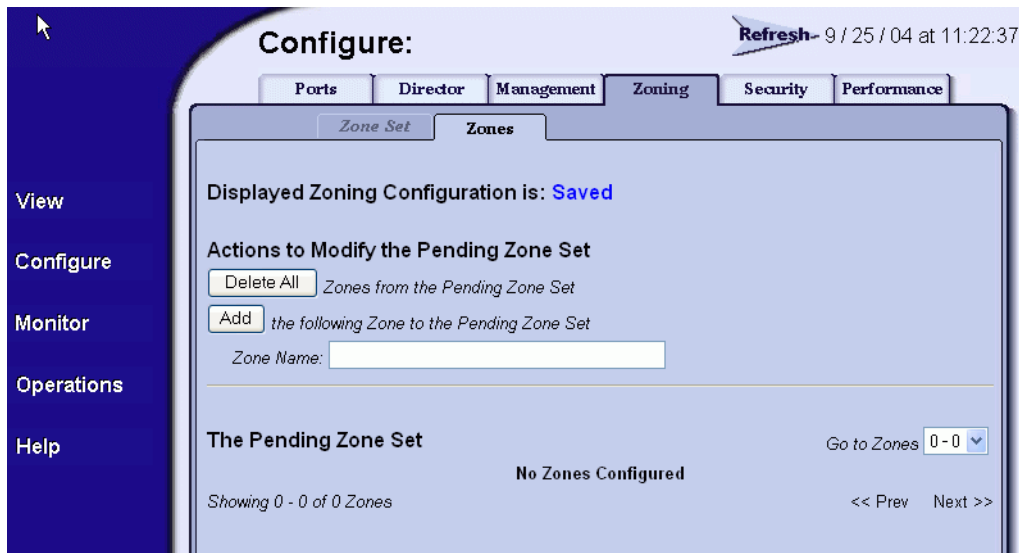


Figure 2-110 Configure Panel (Zoning Page with Zones Tab)

3. Type the zone name and click *Add New Zone*. After the name is validated, the new zone name (**Zone-1**) and an associated *Delete* button appear at the bottom of the page. Note the following:
 - **Save and activate the zone** - Changes to a zone or zoning configuration are not saved and activated on the switch until saved as part of a zone set. Go to [Configure Zone Sets \(SANpilot Interface\)](#) on page 2-124 to perform this function.
 - **Delete all zones** - To delete all configured zones and zone members, click *Delete All Zones*. A confirmation dialog box displays. Click OK to delete all zones.
 - **Delete a single zone** - To delete a single zone and its zone members, click the *Delete* button adjacent to the zone name. A confirmation dialog box displays. Click OK to delete the zone.
 - **Display more zones** - If a zone set contains more than 64 zones, the *Display More Zones* link activates to display subsequent pages. In addition, the *Display Previous Zones* link activates on subsequent displayed pages.

4. To add devices (members) to the zone, click the zone name (**Zone-1**). The *Zoning* page displays with the *Modify Zone* tab selected (Figure 2-111).

Figure 2-111 Configure Panel (Zoning Page with Modify Zone Tab)

5. To rename a configured zone, type the new name in the *Zone* field and click *Rename Zone*. After the name is validated, the zone name is changed.
6. Add or delete zone members as follows:
 - **Add member by attached node WWN** - Select the WWN of an attached device (node) from the *Attached Node World Wide Name* drop-down list and click the adjacent *Add Member* button. The device is added to the zone.
 - **Add member by WWN** - Type the WWN of an attached device in the *World Wide Name* field and click the adjacent *Add Member* button. The device is added to the zone.

- **Add member by domain ID and port number** - Type the domain ID (1 through 31) of the switch in the *Domain ID* field, type the switch port number (0 through 23) to which a device is attached, and click the adjacent *Add Member* button. The device attached to that port is added to the zone.
 - **Delete a member** - To delete a zone member, click the *Delete* button adjacent to the configured zone member (WWN or domain ID and port number) at the bottom of the page. A confirmation dialog box displays. Click OK to delete the zone member.
7. Changes to a zone, zoning configuration, or zone member are not saved and activated on the switch until saved as part of a zone set. Go to [Configure Zone Sets \(SANpilot Interface\)](#) below to perform this function.

Configure Zone Sets (SANpilot Interface)

To configure zone sets at the SANpilot interface:

1. At the *Configure* panel and *Zoning* page, click the *Zone Set* tab. The *Zoning* page displays with the *Zone Set* tab selected ([Figure 2-112](#)).

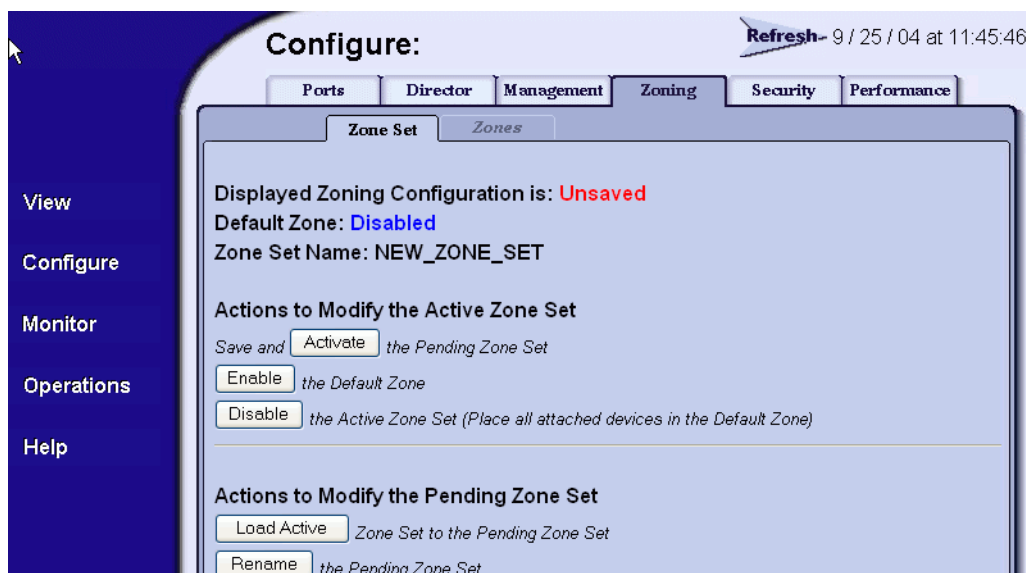


Figure 2-112 Configure Panel (Zoning Page with Zone Set Tab)

2. To create a zone set that incorporates zones and zone members (configured under *Configure Zones (SANpilot Interface)* on page 2-121), type a new zone set name in the *Zone Set Name* field.
3. Click *Save and Activate Zoning Configuration*. After the zone set name is validated, a confirmation dialog box displays.
4. Click *OK* to save and activate the new zone set. The message **Your changes to the Zoning configuration have been successfully activated** appears. Note the following:
 - **Rename zone set** - To rename a zone set, type the new name in the *Zone Set Name* field. Click *Rename Zone Set*. The new zone set name is validated and changed.
 - **Enable or disable default zone** - To toggle (enable or disable) the default zone state, click *Enable Default Zone* or *Disable Default Zone*. Depending on the toggle state, the *Default Zone* field changes to **Enabled** or **Disabled**.
 - **Disable zone set** - To disable the active zone set and place all attached devices in the default zone, click *Disable Zone Set*. A confirmation dialog box displays. Click *OK* to disable the active zone set.
 - **Discard changes** - To discard unsaved changes made to a zone set configuration and revert to a saved zoning configuration, click *Discard Changes*. A confirmation dialog box displays. Click *OK* to discard the changes.

Task 23: Connect Switch to a Fabric Element (Optional)

To provide fabric-attached Fibre channel connectivity for devices connected to the Sphereon 4500 Switch, connect the switch to an expansion port (E_Port) of a fabric element (switch or director). Any switch can be used to form this ISL. To connect the Sphereon 4500 Switch to a fabric element and create an ISL:

1. Ensure the fabric element is accessible by the SANpilot interface or defined to the SAN management application. If the fabric element must be defined, refer to the appropriate switch or director installation manual for instructions.
2. Ensure the preferred domain ID for the Sphereon 4500 Switch is unique and does not conflict with the ID of another switch or director participating in the fabric.

- If the domain ID must be changed from the SANpilot interface, refer to [Task 4: Configure the Switch at the SANpilot Interface \(Optional\)](#) on page 2-13.
 - If the domain ID must be changed from the management server, refer to [Task 19: Configure the Sphereon 4500 Element Manager Application](#) on page 2-88.
3. Ensure the R_A_TOV and E_D_TOV values for the Sphereon 4500 Switch are identical to the values for all switches or directors participating in the fabric.
 - If the values must be changed from the SANpilot interface, refer to [Task 4: Configure the Switch at the SANpilot Interface \(Optional\)](#).
 - If the values must be changed from the management server, refer to [Task 19: Configure the Sphereon 4500 Element Manager Application](#) on page 2-88.
 4. Route a multimode or singlemode fiber-optic cable (depending on the type of transceiver installed) from a customer-specified E_Port of the fabric element to the front of the switch.
 5. Connect the director-attached fiber-optic cable to a Sphereon 4500 Switch port as directed by the customer.
 6. If the switch is managed by a management server, go to [step 7](#). If the switch is managed by the SANpilot interface:
 - a. At the *Configure* panel, select the *View* option at the left side of the panel. The *View* panel opens with the *Switch* page displayed.
 - b. Double-click the graphical port connector used for the fabric ISL (connected in [step 5](#)).
 - c. The *View* panel opens with the *Port Properties* page displayed. Port properties appear for the selected port.
 - d. Ensure the *Operational State* field displays **Online** and the *Reason* field displays **N/A** or is blank. If an ISL segmentation or other problem is indicated, go to [MAP 0000: Start MAP](#) on page 3-6 to isolate the problem. If no problems are indicated, installation tasks are complete.
 7. At the SAN management application's physical map, right-click the Sphereon 4500 product icon, then select *Element Manager* from the pop-up menu.

8. If required, click the *Hardware* tab. The *Hardware View* displays.
9. Double-click the graphical port connector used for the fabric ISL (connected in [step 5](#)). The *Port Properties* dialog box displays ([Figure 2-113](#)).

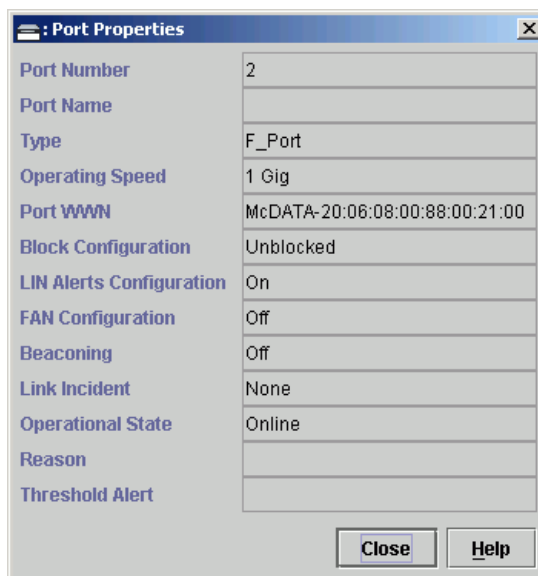


Figure 2-113 Port Properties Dialog Box

10. Ensure the *Link Incident* field displays **None** and the *Reason* field is blank. If an ISL segmentation or other problem is indicated, go to [MAP 0000: Start MAP](#) on page 3-6 to isolate the problem.

Task 24: Register with the McDATA File Center

To complete the installation, register with the McDATA File Center web site to receive e-mail updates and access the following:

- Technical publications.
- Firmware and software upgrades.
- Technical newsletters.
- Release notes.

To register with the McDATA File Center:

1. At a PC with Internet access, open the McDATA File Center home page (Figure 2-114). The uniform resource locator (URL) is <http://central.mcddata.com>.

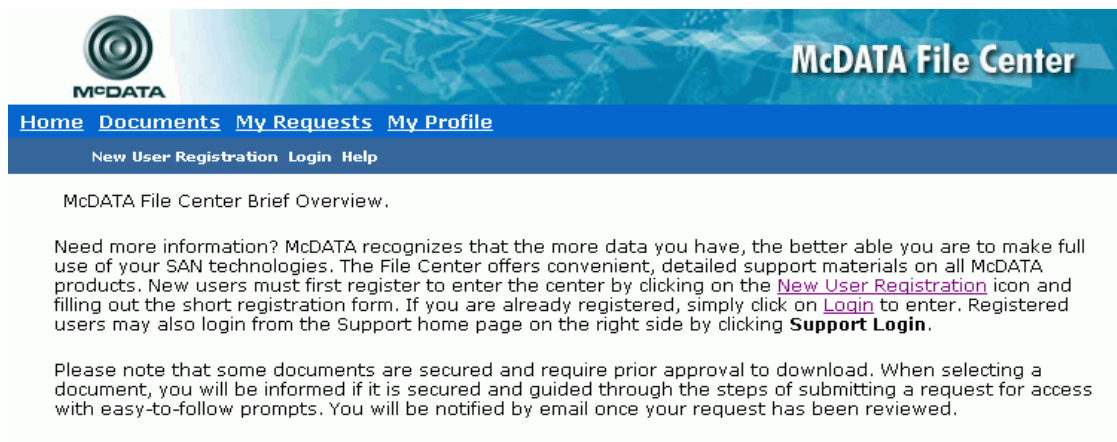


Figure 2-114 McDATA File Center Home Page

2. Select (click) the *New User Registration* option at the top of the home page. The File Center's *New User Registration* page displays (Figure 2-115 on page 2-129). Use the registration page to input required and optional user information. The following information is required:
 - Password.
 - Verify password.
 - First name.
 - Last name.
 - E-mail address.
 - Company.
 - Title.
3. Complete the information fields as required and click *Register*. The registration is complete and File Center login information is transmitted to the e-mail address specified on the *New User Registration* page.

Registration: New File Center

Below are a few fields we need you to fill in so that we can better fulfill your request for information. You will only have to do this once and the information will not be released to any other companies. Information requested below will assist us in routing your request to the appropriate SAN Professional.

There are some mandatory fields that have not been filled in yet or are invalid. Please correct them and click the Register button. Field specific errors are shown to the right of the fields.

Basic User Information

In this section we need to collect some basic information about you and how we can contact you.

Password:	<input type="password"/>	Password is required.
Verify Password:	<input type="password"/>	Verify Password is required.
First Name:	<input type="text"/>	First Name is required.
Middle Name:	<input type="text"/>	
Last Name:	<input type="text"/>	Last Name is required.
E-mail Address:	<input type="text"/>	E-mail Address is required.
Company:	<input type="text"/>	Company is required.
Title:	<input type="text"/>	Title is required.
Phone Number:	<input type="text"/>	
Fax Number:	<input type="text"/>	

Register

Figure 2-115 McDATA File Center (New User Registration Page)

- At the browser PC, close the Internet session. If no switch problems are indicated, installation tasks are complete.

This chapter describes diagnostic procedures used by service representatives to fault isolate Sphereon 4500 Fabric Switch problems or failures to the field-replaceable unit (FRU) level. The chapter specifically describes how to perform maintenance analysis procedures (MAPs).

Maintenance Analysis Procedures

Fault isolation and related service procedures are provided through MAPs. The procedures vary depending on the diagnostic information provided. MAPs consist of step-by-step procedures that prompt service personnel for information or describe a specific action to be performed. MAPs provide information to interpret system events, isolate a switch failure to a single FRU, remove and replace the failed FRU, and verify switch operation.

Factory Defaults

[Table 3-1](#) on page 3-2 lists factory-set defaults for Sphereon 4500 Switch passwords (customer and maintenance-level), and the switch's Internet Protocol (IP) address, subnet mask, and gateway address.

Quick Start

Table 3-1 Factory-Set Defaults

Item	Default
Customer password	password
Maintenance password	level-2
IP address	10.1.1.10
Subnet mask	255.0.0.0
Gateway address	0.0.0.0

[Table 3-2](#) lists and summarizes the MAPs. Fault isolation normally begins at [MAP 0000: Start MAP](#) on page 3-6.

Table 3-2 MAP Summary

MAP	Page
MAP 0000: Start MAP	3-6
MAP 0100: Power Distribution Analysis	3-30
MAP 0200: POST Failure Analysis	3-38
MAP 0300: Server Application Problem Determination	3-41
MAP 0400: Loss of Server Communication	3-51
MAP 0500: FRU Failure Analysis	3-68
MAP 0600: Port Failure and Link Incident Analysis	3-74
MAP 0700: Fabric, ISL, and Segmented Port Problem Determination	3-93
MAP 0800: Server Hardware Problem Determination	3-110

[Table 3-3](#) on page 3-3 lists event codes and the corresponding MAP references. The table provides a quick start guide if an event code is readily available.

Table 3-3 Event Codes versus Maintenance Action

Event Code	Explanation	Action
011	Login Server database invalid.	Go to MAP 0700 .
021	Name Server database invalid.	Go to MAP 0700 .
031	SNMP request received from unauthorized community.	Add a community name through the Element Manager application.
051	Management Server database invalid.	Go to MAP 0700 .
052	Management Server internal error.	Go to MAP 0700 .
061	Fabric Controller database invalid.	Go to MAP 0700 .
062	Maximum interswitch hop count exceeded.	Go to MAP 0700 .
063	Remote switch has too many ISLs.	Go to MAP 0700 .
070	E_Port is segmented.	Go to MAP 0700 .
071	Switch is isolated.	Go to MAP 0700 .
072	E_Port connected to unsupported switch.	Go to MAP 0700 .
073	Fabric initialization error.	Go to Collect Maintenance Data on page 4-44.
074	ILS frame delivery error threshold exceeded.	Go to Collect Maintenance Data on page 4-44.
080	Unauthorized worldwide name.	Go to MAP 0600 .
081	Invalid attachment.	Go to MAP 0600 .
120	Error detected while processing system management command.	Go to Collect Maintenance Data on page 4-44.
121	Zone set activation failed - zone set too large.	Reduce size of zone set and retry.
140	Congestion detected on an ISL.	Go to MAP 0700 .
141	Congestion relieved on an ISL.	No action required.
142	Low BB_Credit detected on an ISL.	Go to MAP 0700 .
143	Low BB_Credit relieved on an ISL.	No action required.
150	Zone merge failure.	Go to MAP 0700 .

Table 3-3 Event Codes versus Maintenance Action (Continued)

Event Code	Explanation	Action
151	Fabric configuration failure.	Go to Collect Maintenance Data on page 4-44.
200	Power supply AC voltage failure.	Go to MAP 0100 .
201	Power supply DC voltage failure.	Go to MAP 0100 .
203	Power supply AC voltage recovery.	No action required.
204	Power supply DC voltage recovery.	No action required.
206	Power supply removed.	Replace FRU.
207	Power supply installed.	No action required.
300	Cooling fan propeller failed.	Go to MAP 0500 .
301	Cooling fan propeller failed.	Go to MAP 0500 .
302	Cooling fan propeller failed.	Go to MAP 0500 .
303	Cooling fan propeller failed.	Go to MAP 0500 .
304	Cooling fan propeller failed.	Go to MAP 0500 .
305	Cooling fan propeller failed.	Go to MAP 0500 .
310	Cooling fan propeller recovered.	No action required.
311	Cooling fan propeller recovered.	No action required.
312	Cooling fan propeller recovered.	No action required.
313	Cooling fan propeller recovered.	No action required.
314	Cooling fan propeller recovered.	No action required.
315	Cooling fan propeller recovered.	No action required.
400	Power-up diagnostic failure.	Go to MAP 0200 .
410	Switch reset.	No action required.
411	Firmware fault.	Go to MAP 0200 .
412	CTP watchdog timer reset.	Go to Collect Maintenance Data on page 4-44.
421	Firmware download complete.	No action required.

Table 3-3 Event Codes versus Maintenance Action (Continued)

Event Code	Explanation	Action
423	CTP firmware download initiated.	No action required.
426	Multiple ECC single-bit errors occurred.	Go to MAP 0500 .
433	Non-recoverable Ethernet fault.	Go to MAP 0500 .
440	Embedded port hardware failed.	Go to MAP 0500 .
442	Embedded port anomaly detected.	No action required.
445	ASIC detected a system anomaly.	No action required.
453	New feature key installed.	No action required.
506	Fibre Channel port failure.	Go to MAP 0600 .
507	Loopback diagnostics port failure.	Go to MAP 0600 .
508	Fibre Channel port anomaly detected.	No action required.
510	SFP optical transceiver hot-insertion initiated.	No action required.
512	SFP optical transceiver nonfatal error.	Go to MAP 0600 .
513	SFP optical transceiver hot-removal completed.	No action required.
514	SFP optical transceiver failure.	Go to MAP 0600 .
523	FL_Port open request failed.	No action required.
524	No AL_PA acquired.	No action required.
525	FL_Port arbitration timeout.	No action required.
581	Implicit incident.	Go to MAP 0600 .
582	Bit error threshold exceeded.	Go to MAP 0600 .
583	Loss of signal or loss of synchronization.	Go to MAP 0600 .
584	Not operational primitive sequence received.	Go to MAP 0600 .
585	Primitive sequence timeout.	Go to MAP 0600 .
586	Invalid primitive sequence received for current link state.	Go to MAP 0600 .
810	High temperature warning (CTP thermal sensor).	Go to MAP 0500 .
811	Critically hot temperature warning (CTP thermal sensor).	Go to MAP 0500 .

MAP 0000: Start MAP

This MAP describes initial fault isolation for the Sphereon 4500. Fault isolation begins at the Internet-connected PC accessing the SANpilot interface, rack-mount management server, customer-supplied server running the Enterprise Fabric Connectivity Manager (EFCM) Lite application, failed switch, or switch-attached host.

1

Prior to fault isolation, acquire the following from the customer:

- A system configuration drawing or planning worksheet that includes the customer-supplied server (accessing the SANpilot interface or running the EFCM Lite application), management server, switch, other McDATA products, and device connections.
- The location of the management server or customer-supplied server and all switches.
- The internet protocol (IP) address, gateway address, and subnet mask for the switch reporting the problem.
- If performing fault isolation using a customer-supplied server accessing the SANpilot interface, the administrator user name and password. Both are case sensitive and required when prompted at the *Username and Password Required* dialog box.
- If performing fault isolation using a customer-supplied server running the EFCM Lite application:
 - The operating system user name and password, required when prompted during any MAP or repair procedure that directs the server to be rebooted.
 - The user name, maintenance password, and server name. All are case sensitive and required when prompted at the *EFCM Log In* dialog box.
- If performing fault isolation using the management server:
 - The Windows 2000 user name and password, required when prompted during any MAP or repair procedure that directs the management server to be rebooted.
 - The user ID and maintenance password. Both are case sensitive and required when prompted at the *SANavigator Log In* or *EFCM Log In* dialog box.

Continue to the next step.

2

Are you at a PC with a web browser (such as Netscape Navigator or Microsoft Internet Explorer), an Internet connection to the switch reporting the problem, and communicating with the switch through the SANpilot interface?

YES NO



Go to [step 19](#).

3

Is the web-browser PC powered on and communicating with the switch through the Internet connection and SANpilot interface?

NO YES



Go to [step 5](#).

4

Boot the web-browser PC.

- a. Power on the PC in accordance with the instructions delivered with the PC. The Windows desktop appears.
- b. Launch the PC browser application by double-clicking the Netscape Navigator icon or Internet Explorer icon at the Windows desktop.
- c. At the *Netsite* field (Netscape Navigator) or *Address* field (Internet Explorer), type **http://xxx.xxx.xxx.xxx**, where **xxx.xxx.xxx.xxx** is the IP address of the switch (obtained in [step 1](#)). The *Username and Password Required* dialog box appears ([Figure 3-1](#)).

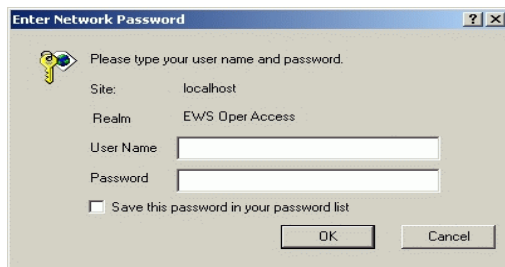


Figure 3-1 Username and Password Required Dialog Box

- d. Type the user name and password obtained in [step 1](#), and click OK. The SANpilot interface opens with the *View* panel displayed ([Figure 3-2](#) on page 3-8).

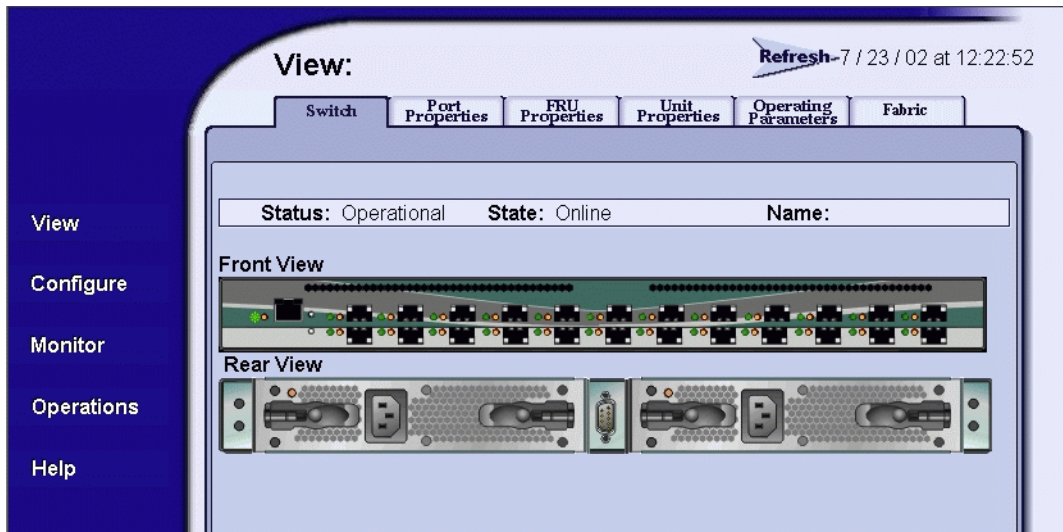


Figure 3-2 View Panel (SANpilot Interface)

Continue to the next step.

5

Does the SANpilot interface appear operational with the *View* panel displayed?

NO YES



Go to [step 10](#).

6

A **Page cannot be found, Unable to locate the server, HTTP 404 - file not found**, or other similar message appears. The message indicates the PC cannot communicate with the switch because:

- The switch-to-PC Internet link could not be established.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch control processor (CTP) card failed.

Continue to the next step.

7

Ensure the switch is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES NO

- ↓ A power distribution problem is indicated. Go to [MAP 0100: Power Distribution Analysis](#) on page 3-30. **Exit MAP.**

8

At the front of the switch, inspect the amber **ERR** LED.

Is the LED illuminated?

NO YES

- ↓ A FRU failure or link incident is indicated. **Go to [step 18](#)** to obtain event codes that identify the failure. **Exit MAP.**

9

A switch-to-PC Internet link problem (Internet too busy or IP address typed incorrectly) is indicated.

- a. Wait approximately five minutes, then attempt to login to the switch again.
- b. At the *Netsite* field (Netscape Navigator) or *Address* field (Internet Explorer), type **http://xxx.xxx.xxx.xxx**, where **xxx.xxx.xxx.xxx** is the IP address of the switch (obtained in [step 1](#)). The *Username and Password Required* dialog box appears ([Figure 3-1](#) on page 3-7).
- c. Type the user name and password obtained in [step 1](#), and click **OK**. If the *View* panel does not display, wait another five minutes and perform this step again.

Does the SANpilot interface appear operational with the *View* panel displayed?

YES NO

↓ Perform switch fault isolation at the management server or customer-supplied server running the EFCM Lite application.
Go to step 20.

10

At the *View* panel, inspect the *Status* field.

Does the switch status indicate **Operational**?

NO YES

↓ The switch appears operational. **Exit MAP.**

11

Inspect Fibre Channel port operational states.

- a. At the *View* panel, click the *Port Properties* tab. The *View* panel (*Port Properties* tab) displays with port **0** highlighted (Figure 3-3).

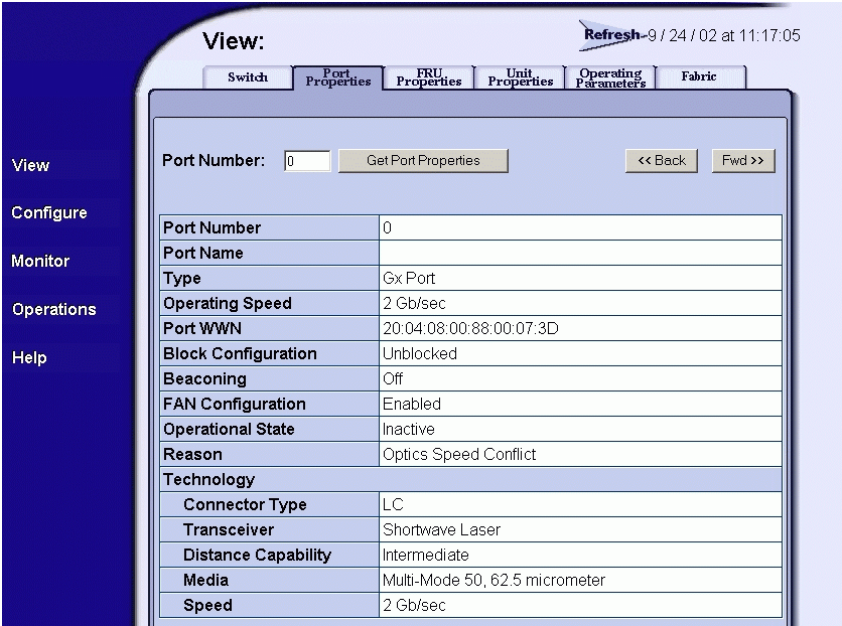


Figure 3-3 View Panel (Port Properties Tab)

- b. Inspect the *Beaconing* and *Operational State* fields.

Does the *Beaconing* field display an **On** message?

YES NO

↓ **Go to [step 13](#).**

12

Port beaconing is enabled.

- a. Consult the customer and next level of support to determine the reason port beaconing is enabled.
- b. Disable port beaconing:
 - 1. At the *View* panel, select *Operations* at the left side of the panel. The *Operations* panel opens with the *Port Beaconing* page displayed.
 - 2. Click the *Beaconing State* check box for the port. The check mark disappears and port beaconing is disabled.
 - 3. Return to the *View* panel (*Port Properties* tab).

Continue to the next step.

13

At the *View* panel, does the *Operational State* field display a **Segmented** message?

NO YES

↓ Port segmentation is indicated. **Go to [step 18](#)** to obtain event codes. If no event codes are found, go to [MAP 0700: Fabric, ISL, and Segmented Port Problem Determination](#) on page 3-93. **Exit MAP.**

14

At the *View* panel, does the *Operational State* field display a message indicating a port problem?

NO YES

↓ **Go to [step 18](#)** to obtain event codes. If no event codes are found, go to [MAP 0600: Port Failure and Link Incident Analysis](#) on page 3-74. **Exit MAP.**

15

Repeat [step 11](#) through [step 14](#) for each remaining Fibre Channel port for which a problem is suspected (ports **0** through **23**).

Is a problem indicated for any of the ports?

NO **YES**



Go to [step 18](#) to obtain event codes. If no event codes are found, go to [MAP 0600: Port Failure and Link Incident Analysis](#) on page 3-74. **Exit MAP.**

16

Inspect power supply operational states.

- a. At the *View* panel, click the *FRU Properties* tab. The *View* panel (*FRU Properties* tab) displays ([Figure 3-4](#)).

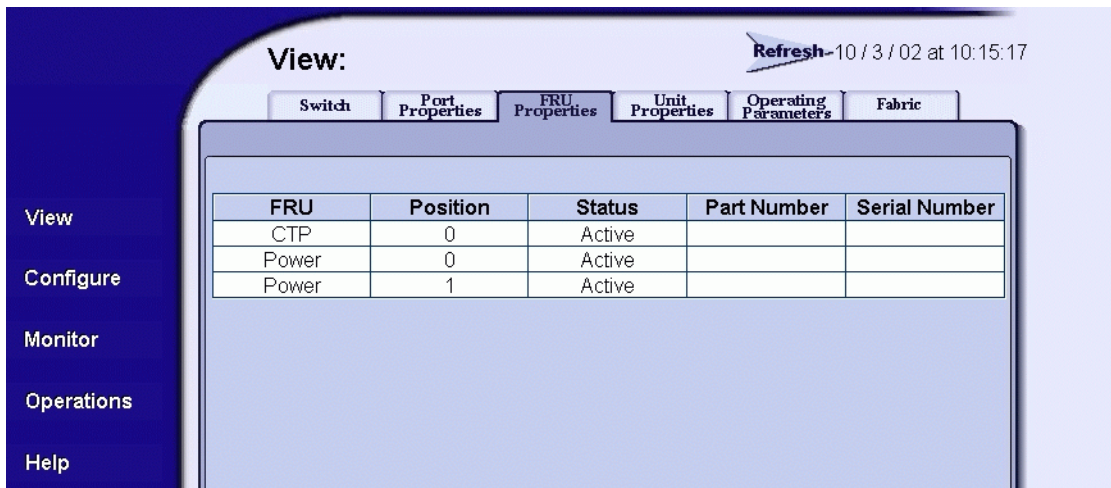


Figure 3-4 View Panel (FRU Properties Tab)

- b. Inspect the *Status* fields for both power supplies.

Does the *Status* field display a **Failed** message for either power supply?

NO **YES**



A power supply failure is indicated. **Go to [step 18](#)** to obtain event codes. If no event codes are found, go to [MAP 0100: Power Distribution Analysis](#) on page 3-30. **Exit MAP.**

17

Inspect the *Status* fields for switch FRUs.

Does the *State* field display a **Failed** message for any of the FRUs?

YES NO

↓ The switch appears operational. **Exit MAP.**

A FRU failure is indicated. Continue to the next step to obtain event codes. If no event codes are found, go to [MAP 0500: FRU Failure Analysis](#) on page 3-68. **Exit MAP.**

18

Obtain event codes from the SANpilot event log.

NOTE: If multiple event codes are found, note all codes and associated severity levels. Record the date, time, and listed sequence, and determine if the codes are related to the reported problem. Begin fault isolation with the most recent event code with the highest severity level. Other codes may accompany this event code, or may indicate a normal indication after a problem is recovered.

- At the *View* panel, select *Monitor* at the left side of the panel. The *Monitor* panel opens with the *Port List* page displayed.
- At the *Monitor* panel, click the *Log* tab. The *Monitor* panel (*Log* tab) displays ([Figure 3-5](#)).

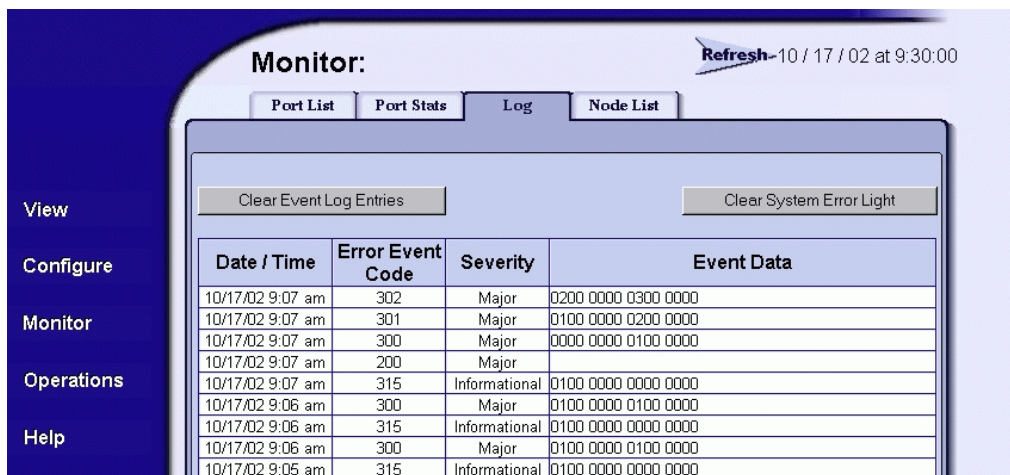


Figure 3-5 Monitor Panel (Log Tab)

- c. Record the event code, date, time, and severity (*Informational, Minor, Major, or Severe*).
- d. Record all event codes that may relate to the reported problem.

Were one or more event codes found?

NO YES

↓ **Go to [Table 3-3](#) on page 3-3 to interpret event codes. Exit MAP.**

Return to [step 1](#) and perform fault isolation again. If this is the second time at this step, contact the next level of support. **Exit MAP.**

19

Are you at the management server or customer-supplied server running the EFCM Lite application?

YES NO

↓ **Go to [step 39](#).**

20

Did the management server or customer-supplied server lock up or crash and:

- Display an application warning or error message, or
- Not display an application warning or error message, or
- Display a *Dr. Watson for Windows 2000* dialog box?

NO YES

↓ A management server or customer-supplied server application problem is indicated. Event codes are not recorded. Go to [MAP 0300: Server Application Problem Determination](#) on page 3-41. **Exit MAP.**

21

Did the management server or customer-supplied server crash and display a blue screen with the system dump file in hexadecimal format (blue screen of death)?

NO YES

↓ A management server or customer-supplied server application problem is indicated. Event codes are not recorded. Go to [MAP 0300: Server Application Problem Determination](#) on page 3-41. **Exit MAP.**

22

Is the SAN management application (SANavigator 4.0 or EFCM 8.0) active?

NO **YES**



Go to [step 24](#).

23

Reboot the management server or customer-supplied server. If the customer-supplied server does not use the Windows 2000 operating system, refer to the supporting documentation to reboot the server.

- a. At the Windows 2000 desktop, click *Start* at the left side of the task bar (bottom of the desktop), then select *Shut Down*. The *Shut Down Windows* dialog box displays ([Figure 3-6](#)).



Figure 3-6 Shut Down Windows Dialog Box

- b. Select the *Shut Down* option from the list box and click *OK*. The management server powers down.
- c. Wait approximately 30 seconds and press the power (⏻) button on the liquid crystal display (LCD) panel to power on the server and perform power-on self-tests (POSTs). During POSTs:

1. The green LCD panel illuminates.
2. The green hard disk drive (**HDD**) LED blinks momentarily, and processor speed and random-access memory information display momentarily at the LCD panel.
3. After a few seconds, the LCD panel displays the following message pertaining to boot sequence selection ([Figure 3-7](#)):



Boot from LAN?
Press <Enter>

Figure 3-7 LCD Panel During Boot Sequence

4. Ignore the message. After ten seconds, the server performs the boot sequence from the basic input/output system (BIOS). During the boot sequence, the server performs additional POSTs and displays the following operational information at the LCD panel:
 - Host name.
 - System date and time.
 - LAN 1 and LAN 2 IP addresses.
 - Fan 1, fan 2, fan 3, and fan 4 rotational speed.
 - Central processing unit (CPU) temperature.
 - Hard disk capacity.
 - Virtual and physical memory capacity.
- d. After successful POST completion, the LCD panel displays a **Welcome!!** message, then continuously cycles through and displays server operational information.
- e. After rebooting the server at the LCD panel, log on to the management server's Windows 2000 desktop through a LAN connection to a browser-capable PC. Refer to [Access the Management Server Desktop](#) on page 2-55 for instructions. The SAN management application starts and the *SANavigator Log In* or *EFCM Log In* dialog box displays ([Figure 3-8](#) on page 3-17).

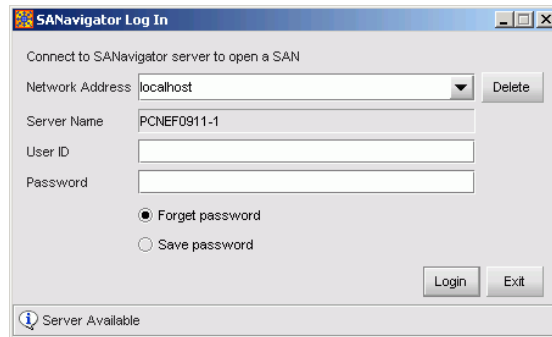


Figure 3-8 SANavigator Login or EFCM Login Dialog Box

- f. Type a user ID and password (obtained in [step 1](#), and both are case sensitive), and click *Login*. The SAN management application opens and the SANavigator or EFCM main window displays ([Figure 3-9](#)).

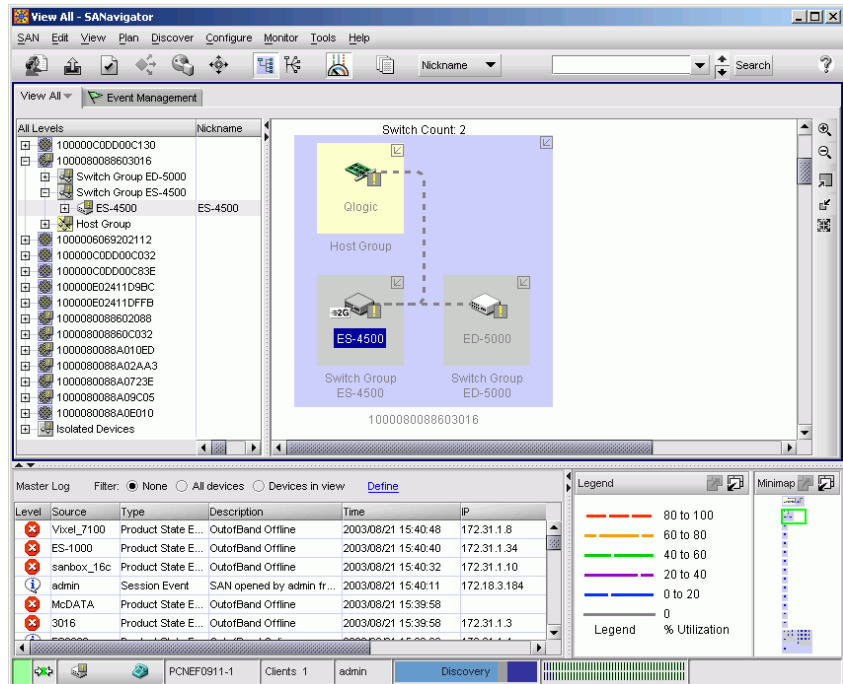


Figure 3-9 Main Window (SANavigator or EFCM)

Did the main window display and does the SAN management application appear operational?

YES NO



A management server or customer-supplied server hardware problem is indicated. Event codes are not recorded. Go to [MAP 0800: Server Hardware Problem Determination](#) on page 3-110. **Exit MAP.**

24

Inspect the status symbol associated with the Sphereon 4500 Switch at the main window's physical map or product list. The symbol shows the status of switch or the status of the link between the management server or customer-supplied server and switch as follows:

- No status symbol indicates that the switch is operational.
- A yellow triangle indicates that the switch is operating in degraded mode.
- A red diamond indicates that the switch is not operational.
- A grey square with yellow exclamation mark indicates that the status of the switch is unknown.

Is a grey square with yellow exclamation mark associated with the icon representing the switch reporting the problem?

YES NO



Go to [step 28](#).

The status symbol indicates the management server or customer-supplied server cannot communicate with the switch because:

- The switch-to-server Ethernet link failed.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP card failed.

Continue to the next step.

25

Ensure the switch is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES NO



A power distribution problem is indicated. **Go to step 38** to obtain event codes. If no event codes are found, go to [MAP 0100: Power Distribution Analysis](#) on page 3-30. **Exit MAP.**

26

At the front of the switch, inspect the amber **ERR** LED.

Is the LED illuminated?

NO YES



A FRU failure or link incident is indicated. **Go to step 38** to obtain event codes that identify the failure. **Exit MAP.**

27

A switch-to-server Ethernet link failure is indicated.

Go to step 38 to obtain event codes. If no event codes are found, go to [MAP 0400: Loss of Server Communication](#) on page 3-51. **Exit MAP.**

28

Is a red diamond (failure indicator) associated with the icon representing the switch reporting the problem?

YES NO



Go to step 30.

29

Right-click the icon representing the switch reporting the problem. A pop-up menu appears. Select the *Element Manager* option from the menu. The Element Manager application opens and the *Hardware View* displays (Figure 3-10).

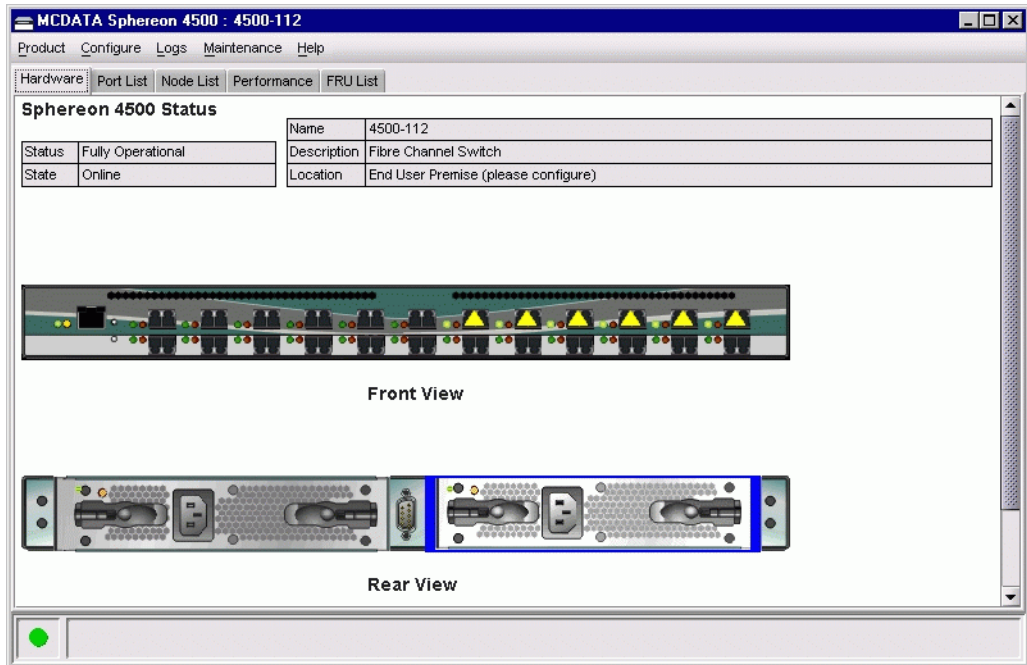


Figure 3-10 Hardware View

At the *Hardware View*:

- Observe that the *Sphereon 4500 Status* table is yellow and the switch status is **NOT OPERATIONAL**.
- Inspect FRUs for a blinking red and yellow diamond (failed FRU indicator) that overlays the FRU graphic.

Do blinking red and yellow diamonds overlay any FRU graphics?

NO **YES**



Failure of one or more FRUs is indicated. **Go to step 38** to obtain event codes. If no event codes are found, go to [MAP 0500: FRU Failure Analysis](#) on page 3-68. **Exit MAP.**

30

Is a yellow triangle (attention indicator) associated with the icon representing the switch reporting the problem?

YES NO



Go to [step 33](#).

31

Right-click the icon representing the switch reporting the problem. A pop-up menu appears. Select the *Element Manager* option from the menu. The Element Manager application opens and the *Hardware View* displays ([Figure 3-10](#) on page 3-20). At the *Hardware View*:

- Observe that the *Sphereon 4500 Status* table is yellow and the switch status is **Minor Failure** or **Redundant Failure**.
- Inspect FRUs for a blinking red and yellow diamond (failed FRU indicator) that overlays the FRU graphic.

Does a blinking red and yellow diamond overlay a power supply graphic?

NO YES



A power supply failure is indicated. **Go to step 38** to obtain event codes. If no event codes are found, go to [MAP 0100: Power Distribution Analysis](#) on page 3-30. **Exit MAP.**

32

Does a blinking red and yellow diamond overlay a port graphic?

NO YES



A port failure is indicated. **Go to step 38** to obtain event codes. If no event codes are found, go to [MAP 0600: Port Failure and Link Incident Analysis](#) on page 3-74. **Exit MAP.**

33

No colored status symbol is associated the icon representing the switch reporting the problem. Although the switch is operational, a minor problem may exist.

Right-click the icon representing the switch reporting the problem. A pop-up menu appears. Select the *Element Manager* option from the menu. The Element Manager application opens and the *Hardware View* displays ([Figure 3-10](#) on page 3-20). At the *Hardware View*:

- Inspect the switch for a yellow triangle that overlays the FRU graphic and indicates FRU beaconing is enabled.
- Inspect ports for a yellow triangle (attention indicator) that overlays the port graphic.

Does a yellow triangle overlay the switch or FRU graphic?

YES NO



Go to [step 35](#).

34

Beaconing is enabled for the FRU.

- a. Consult the customer and next level of support to determine the reason FRU beaconing is enabled.
- b. Disable FRU beaconing.
 1. At the *Hardware View* ([Figure 3-10](#) on page 3-20), right-click the FRU graphic. A pop-up menu appears.
 2. Click the *Enable Beaconing* option. The check mark disappears from the box adjacent to the option, and FRU beaconing is disabled.

Was FRU beaconing enabled because FRU failure or degradation was suspected?

YES NO



The switch appears operational. **Exit MAP.**

Go to [step 20](#) and perform fault isolation again (through the management server or customer-supplied server).

35

Does a yellow triangle (attention indicator) overlay a port graphic?

YES NO



Go to [step 37](#).

36

Inspect the port state and LED status for all ports with an attention indicator.

- a. Double-click a port to open the *Port Properties* dialog box ([Figure 3-11](#) on page 3-23).

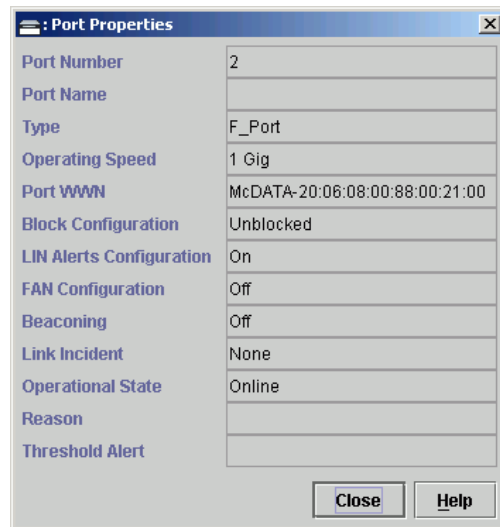


Figure 3-11 Port Properties Dialog Box

b. Inspect the *Operational State* field.

Does the *Operational State* field display a **Segmented E_Port** message?

NO YES



Expansion port (E_Port) segmentation is indicated. **Go to step 38** to obtain event codes. If no event codes are found, go to [MAP 0700: Fabric, ISL, and Segmented Port Problem Determination](#) on page 3-93. **Exit MAP.**

A message displays indicating a link incident problem. **Go to step 38** to obtain event codes. If no event codes are found, go to [MAP 0600: Port Failure and Link Incident Analysis](#) on page 3-74. **Exit MAP.**

37

A link incident may have occurred, but the LIN alerts option is not enabled for the port and the attention indicator does not appear.

At the *Hardware View*, click *Logs* and select *Link Incident Log*. The *Link Incident Log* displays ([Figure 3-12](#) on page 3-24).

Date/Time	port	Link Incident
2003/09/03 14:59:10	9	NOS Received
2003/09/03 14:59:04	11	NOS Received
2003/09/03 14:58:37	9	NOS Received

Figure 3-12 Link Incident Log

If a link incident occurred, the affected port number is listed with one of the following messages.

Link interface incident - implicit incident.

Link interface incident - bit-error threshold exceeded.

Link failure - loss of signal or loss of synchronization.

Link failure - not-operational primitive sequence (NOS) received.

Link failure - primitive sequence timeout.

Link failure - invalid primitive sequence received for the current link state.

Did one of the listed messages appear in the *Link Incident Log*?

YES NO

↓ The switch appears operational. **Exit MAP.**

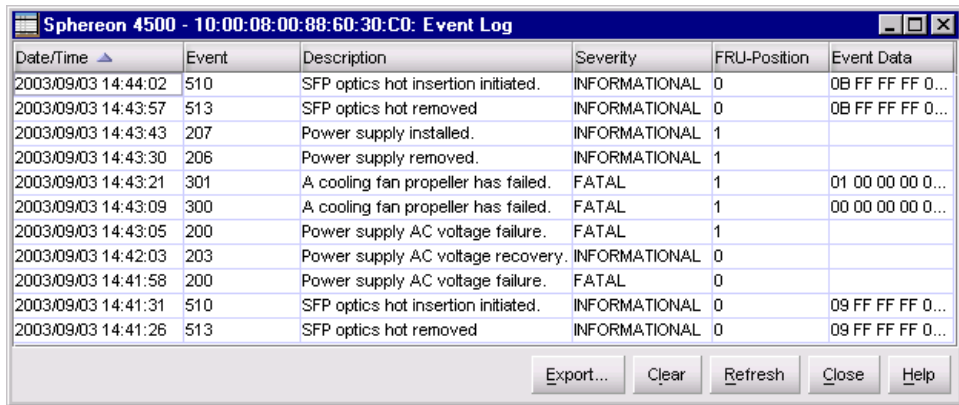
A link incident problem is indicated. Continue to the next step to obtain event codes. If no event codes are found, go to [MAP 0700: Fabric, ISL, and Segmented Port Problem Determination](#) on page 3-93. **Exit MAP.**

38

Obtain event codes from the Sphereon 4500 *Event Log*.

NOTE: If multiple event codes are found, note all codes and associated severity levels. Record the date, time, and listed sequence, and determine if the codes are related to the reported problem. Begin fault isolation with the most recent event code with the highest severity level. Other codes may accompany this event code, or may indicate a normal indication after a problem is recovered.

- a. At the *Hardware View*, click *Logs* and select *Event Log*. The *Event Log* displays (Figure 3-13).



Date/Time	Event	Description	Severity	FRU-Position	Event Data
2003/09/03 14:44:02	510	SFP optics hot insertion initiated.	INFORMATIONAL	0	0B FF FF FF 0...
2003/09/03 14:43:57	513	SFP optics hot removed	INFORMATIONAL	0	0B FF FF FF 0...
2003/09/03 14:43:43	207	Power supply installed.	INFORMATIONAL	1	
2003/09/03 14:43:30	206	Power supply removed.	INFORMATIONAL	1	
2003/09/03 14:43:21	301	A cooling fan propeller has failed.	FATAL	1	01 00 00 00 0...
2003/09/03 14:43:09	300	A cooling fan propeller has failed.	FATAL	1	00 00 00 00 0...
2003/09/03 14:43:05	200	Power supply AC voltage failure.	FATAL	1	
2003/09/03 14:42:03	203	Power supply AC voltage recovery.	INFORMATIONAL	0	
2003/09/03 14:41:58	200	Power supply AC voltage failure.	FATAL	0	
2003/09/03 14:41:31	510	SFP optics hot insertion initiated.	INFORMATIONAL	0	09 FF FF FF 0...
2003/09/03 14:41:26	513	SFP optics hot removed	INFORMATIONAL	0	09 FF FF FF 0...

Export... Clear Refresh Close Help

Figure 3-13 Event Log

- b. Record the event code, date, time, and severity (*Informational*, *Minor*, *Major*, *Severe*, or *Fatal*).
- c. Record all event codes that may relate to the reported problem.

Were one or more event codes found?

NO **YES**



Go to Table 3-3 on page 3-3 to interpret event codes.
Exit MAP.

Return to step 1 and perform fault isolation again. If this is the second time at this step, contact the next level of support. **Exit MAP.**

39

Are you at the switch reporting the problem?

YES **NO**

↓ **Go to [step 51](#).**

40

Is the green **PWR** LED at the switch front bezel illuminated?

NO **YES**

↓ **Go to [step 45](#).**

41

Is the switch connected to facility AC power and powered on?

NO **YES**

↓ **Go to [step 44](#).**

42

Connect the switch to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES **NO**

↓ A power distribution problem is indicated. **Go to [step 38](#)** to obtain event codes. If no event codes are found, go to [MAP 0100: Power Distribution Analysis](#) on page 3-30. **Exit MAP.**

43

Is the green **PWR** LED at the switch front bezel illuminated?

NO **YES**

↓ **Go to [step 45](#).**

A faulty **PWR** LED is indicated, but switch and Fibre Channel port operation is not disrupted. The LED is connected to CTP card circuitry, and if this problem is a concern to the customer, the switch must be replaced. **Exit MAP.**

44

Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES NO

- ↓ A power distribution problem is indicated. **Go to step 38** to obtain event codes. If no event codes are found, go to [MAP 0100: Power Distribution Analysis](#) on page 3-30. **Exit MAP.**

A faulty **PWR** LED is indicated, but switch and Fibre Channel port operation is not disrupted. The LED is connected to CTP card circuitry, and if this problem is a concern to the customer, the switch must be replaced. **Exit MAP.**

45

Is the amber **ERR** LED at the switch front bezel blinking?

YES NO

- ↓ **Go to step 47.**

46

Unit beaconing is enabled for the switch.

- a. Consult the customer and next level of support to determine the reason unit beaconing is enabled.
- b. Disable unit beaconing.
 1. At the *Hardware View* ([Figure 3-10](#) on page 3-20), right-click the front bezel graphic (away from a FRU). A pop-up menu appears.
 2. Click the *Enable Unit Beaconing* option. The check mark disappears from the box adjacent to the option, and unit beaconing is disabled.

Was unit beaconing enabled because switch failure or degradation was suspected?

YES NO

↓ The switch appears operational. **Exit MAP.**

Go to [step 39](#) and perform fault isolation again (at the switch).

47

Is the amber **ERR** LED at the switch front bezel illuminated?

YES NO

↓ The switch appears operational. Verify switch operation at the management server or customer-supplied server running the EFCM Lite application. **Go to [step 20](#).**

48

Check FRUs for failure symptoms.

Are any amber LEDs associated with Fibre Channel ports illuminated?

NO YES

↓ A Fibre Channel port failure is indicated. **Go to [step 38](#)** to obtain event codes. If no event codes are found, go to [MAP 0600: Port Failure and Link Incident Analysis](#) on page 3-74. **Exit MAP.**

49

Is the amber **ERR** LED at the front of the switch illuminated?

NO YES

↓ A FRU failure or link incident is indicated. **Go to [step 38](#)** to obtain event codes that identify the failure. **Exit MAP.**

50

Is the amber LED on a power supply illuminated?

NO YES

↓ A power supply failure is indicated. **Go to [step 38](#)** to obtain event codes. If no event codes are found, go to [MAP 0100: Power Distribution Analysis](#) on page 3-30. **Exit MAP.**

The switch appears operational. **Exit MAP.**

51

You are at the console of an open systems interconnection (OSI) server attached to the switch reporting the problem. If an incident occurs on the Fibre Channel link between the switch and server, a link incident record is generated and sent to the server using the reporting procedure defined in T11/99-017v0.

Was a link incident record generated and sent to the switch-attached OSI server?

YES NO

- ↓ Perform switch fault isolation at the management server or customer-supplied server running the EFCM Lite application.
Go to [step 20](#).

52

The link incident record provides the attached switch port number(s) and one or more of the following event codes and messages. Record all event codes that may relate to the reported problem.

581 - Link interface incident - implicit incident.

582 - Link interface incident - bit-error threshold exceeded.

583 - Link failure - loss of signal or loss of synchronization.

584 - Link failure - not-operational primitive sequence (NOS) received.

585 - Link failure - primitive sequence timeout.

586 - Link failure - invalid primitive sequence received for the current link state.

Were one or more event codes found?

YES NO

- ↓ Perform switch fault isolation at the management server or customer-supplied server running the EFCM Lite application.
Go to [step 20](#).

Go to [Table 3-3](#) on page 3-3 to interpret event codes. Exit MAP.

MAP 0100: Power Distribution Analysis

This MAP describes fault isolation for the switch power distribution system, including defective AC power cords or redundant power supplies.

1

Was an event code **200** or **201** observed at the SANpilot event log or at the Sphereon 4500 *Event Log* (management server)?

YES NO



Go to [step 9](#).

2

[Table 3-4](#) lists event codes, brief explanations of the codes, and the associated steps that describe fault isolation procedures.

Table 3-4 MAP 100 Event Codes

Event Code	Explanation	Action
200	Power supply AC voltage failure.	Go to step 3 .
201	Power supply DC voltage failure.	Go to step 3 .

3

Have the customer inspect and verify that facility power is within specifications. These specifications are:

- One single-phase connection for each power supply.
- Input power between 100 and 240 VAC, and at least 5 amps.
- Input frequency between 47 and 63 Hz.

Is facility power within specifications?

YES NO



Ask the customer to correct the facility power problem. When facility power is corrected, continue to the next step.

4

A redundant power supply is disconnected from facility power, not properly installed, or has failed. Verify the power supply is connected to facility power.

- a. Ensure the AC power cord associated with the power supply (**PS0** or **PS1**) is connected to the rear of the switch and a facility power receptacle. If not, connect the cord as directed by the customer.
- b. Ensure the associated facility circuit breaker is on. If not, ask the customer set the circuit breaker on.
- c. Ensure the AC power cord is not damaged. If damaged, replace the cord.

Was a corrective action performed?

YES NO

↓ **Go to [step 6](#).**

5

Verify redundant power supply operation.

- a. Inspect the power supply and ensure the amber LED is extinguished.
- b. At the management server's *Hardware View* ([Figure 3-10](#) on page 3-20), observe the graphic representing the power supply and ensure a failure symbol (blinking red and yellow diamond) does not appear.

Is a failure indicated?

YES NO

↓ The switch appears operational. **Exit MAP.**

6

Ensure the indicated power supply is correctly installed and seated in the switch. If required, partially remove and reseal the power supply. Refer to [RRP 2: Redundant Power Supply](#) on page 5-6.

Was a corrective action performed?

YES NO

↓ **Go to [step 8](#).**

7

Verify redundant power supply operation.

- a. Inspect the power supply and ensure the amber LED is extinguished.
- b. At the management server's *Hardware View* ([Figure 3-10](#) on page 3-20), observe the graphic representing the power supply and ensure a failure symbol (blinking red and yellow diamond) does not appear.

Is a failure indicated?

YES NO

↓ The switch appears operational. **Exit MAP.**

8

Visual inspection or an event code **200** or **201** indicates one or both power supplies must be removed and replaced. Refer to [RRP 2: Redundant Power Supply](#) on page 5-6.

- This procedure is concurrent and can be performed while switch power is on.
- Perform the data collection procedure as part of FRU removal and replacement.
- If multiple power supply failures occurred, connect the switch to facility AC power after both power supplies are replaced.

ATTENTION ! Do not remove a power supply unless a replacement FRU is immediately available. To avoid product overheating, a removed power supply must be replaced within five minutes.

Did power supply replacement solve the problem?

NO YES

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

9

Is fault isolation being performed at the switch?

YES NO



Fault isolation is being performed at the SANpilot interface, management server, or customer-supplied server. **Go to step 18.**

10

Verify the switch is connected to facility power and is powered on.

- a. Ensure the AC power cord associated with the power supply (**PS0** or **PS1**) is connected to the rear of the switch and a facility power receptacle. If not, connect the cord as directed by the customer.
- b. Ensure the associated facility circuit breaker is on. If not, ask the customer set the circuit breaker on.
- c. Ensure the AC power cord is not damaged. If damaged, replace the cord.

Continue to the next step.

11

Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES NO



Go to step 13.

12

Does inspection of a power supply indicate a failure (amber LED is illuminated)?

NO YES



A redundant power supply failed. **Go to step 8.**

The switch appears operational. **Exit MAP.**

13

The switch AC power distribution system failed. Possible causes include failure of:

- Both power supplies.
- The CTP card.

Does inspection of both power supplies indicate a dual failure (amber LED illuminated on each power supply)?

YES NO

- ↓ One or both power supplies appear operational, but a power distribution failure through the CTP card is indicated.
Go to [step 17](#).

14

Ensure both power supplies are correctly installed and seated in the switch. If required, partially remove and reseal the power supplies. Refer to [RRP 2: Redundant Power Supply](#) on page 5-6.

Was a corrective action performed?

YES NO

- ↓ **Go to [step 16](#).**

15

Verify operation of both power supplies.

- a. Inspect the power supplies and ensure the amber LEDs are extinguished.
- b. At the management server's *Hardware View* ([Figure 3-10](#) on page 3-20), observe the graphics representing the power supplies and ensure a failure symbol (blinking red and yellow diamond) does not appear.

Is a dual power supply failure still indicated?

YES NO

- ↓ The switch appears operational. **Exit MAP.**

16

Both power supplies failed and must be removed and replaced. Refer to [RRP 2: Redundant Power Supply](#) on page 5-6.

- Perform the data collection procedure as part of FRU removal and replacement.
- Connect the switch to facility AC power after both power supplies are replaced.

Did dual power supply replacement solve the problem?

NO YES

↓ The switch appears operational. **Exit MAP.**

A dual power supply failure is not confirmed. Replace both original power supplies to avoid the cost of expending replacement FRUs.

Continue to the next step.

17

One or both power supplies appear operational, but the CTP card is not receiving DC power. The in-card circuit breaker may have tripped due to a power surge, or the CTP card failed.

Disconnect both power cords, then reconnect the power cords (power cycle the switch) to reset the CTP card.

Did power cycling the switch solve the problem?

NO YES

↓ The switch appears operational. **Exit MAP.**

Analysis for a CTP card failure is not described in this MAP. Go to [MAP 0000: Start MAP](#) on page 3-6. **Exit MAP.**

18

Is fault isolation being performed at the SANpilot interface?

YES NO

↓ Fault isolation is being performed at the management server or customer-supplied server. **Go to step 23.**

19

Does the SANpilot interface appear operational?

NO YES

↓ **Go to step 22.**

20

A **Page cannot be found, Unable to locate the server, HTTP 404 - file not found**, or other similar message appears. The message indicates the PC cannot communicate with the switch because:

- The switch-to-PC Internet link could not be established.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP card failed.

Continue to the next step.

21

Ensure the switch reporting the problem is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES NO



Go to [step 13](#).

Analysis for an Ethernet link or a CTP failure is not described in this MAP. Go to [MAP 0000: Start MAP](#) on page 3-6. If this is the second time at this step, contact the next level of support. **Exit MAP.**

22

Inspect power supply operational states at the SANpilot interface.

- a. At the *View* panel, click the *FRU Properties* tab. The *View* panel (*FRU Properties* tab) displays.
- b. Inspect the *Status* fields for both power supplies.

Does the *Status* field display a **Failed** message for either power supply?

NO YES



A redundant power supply failed. **Go to [step 8](#).**

The switch appears operational. **Exit MAP.**

23

At the management server's *Hardware View* (Figure 3-10 on page 3-20), does a yellow triangle appear at the alert panel and a blinking red and yellow diamond (failed FRU indicator) appear to overlay a power supply graphic?

NO **YES**



A redundant power supply failed. **Go to step 8.**

24

At the *Hardware View*, does a grey square appear at the alert panel, a **No Link** status appear at the *Sphereon 4500 Status* table, and graphical FRUs appear uninstalled?

YES **NO**



A green circle appears at the alert panel and the switch appears operational. **Exit MAP.**

The grey square indicates the management server or customer-supplied server cannot communicate with the switch because:

- The switch-to-server Ethernet link failed.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP card failed.

Continue to the next step.

25

Ensure the switch is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES **NO**



Go to step 13.

Analysis for an Ethernet link or a CTP failure is not described in this MAP. Go to [MAP 0000: Start MAP](#) on page 3-6. If this is the second time at this step, contact the next level of support. **Exit MAP.**

MAP 0200: POST Failure Analysis

When the switch is powered on, it performs a series of power-on self-tests (POSTs). When POSTs complete, the switch performs an initial program load (IPL) that loads firmware and brings the unit online. This MAP describes fault isolation for problems that may occur during the POST/IPL process.

If an error occurs, the POST/IPL process continues in an attempt to initialize the switch and bring it online. An event code **400** displays when the switch completes the POST/IPL process.

1

Ensure the switch is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES NO



An AC power distribution problem is indicated, and analysis for the failure is not described in this MAP. Go to [MAP 0100: Power Distribution Analysis](#) on page 3-30. **Exit MAP.**

2

Was an event code **400** or **411** observed at the SANpilot event log or at the Sphereon 4500 *Event Log* (management server)?

YES NO



Analysis for the failure is not described in this MAP. Go to [MAP 0000: Start MAP](#) on page 3-6. **Exit MAP.**

3

[Table 3-5](#) on page 3-39 lists event codes, brief explanations of the codes, and the associated steps that describe fault isolation procedures.

Table 3-5 MAP 200 Event Codes

Event Code	Explanation	Action
400	Power-up diagnostic failure.	Go to step 4 .
411	Firmware fault.	Go to step 8 .

4

POST/IPL diagnostics detected a FRU failure as indicated by event code **400** with supplementary event data.

- At the SANpilot event log or the Sphereon 4500 *Event Log*, examine the first two bytes (**0** and **1**) of event data associated with event code **400**.
- Byte **0** is a FRU code that indicates the failed component. Byte **1** is the slot number of the failed FRU (**00** for a nonredundant FRU, and **00** or **01** for redundant FRUs).

[Table 3-6](#) lists byte **0** FRU codes and associated steps that describe fault isolation procedures.

Table 3-6 MAP 200 Byte 0 FRU Codes

Byte 0	Failed FRU	Action
02	CTP card.	Go to step 5 .
05	Fan module.	Go to step 6 .
06	Power supply.	Go to step 7 .

5

The CTP card failed POSTs (as indicated by FRU code **02**). Replace the switch. **Exit MAP.**

6

A fan module failed POSTs (as indicated by FRU code **05**) and the power supply containing the fan must be removed and replaced. Refer to [RRP 2: Redundant Power Supply](#) on page 5-6.

- This procedure is concurrent and can be performed while switch power is on.
- Perform the data collection procedure as part of FRU removal and replacement.
- If multiple power supply failures occurred, connect the switch to facility AC power after both power supplies are replaced.

ATTENTION ! Do not remove a power supply unless a replacement FRU is immediately available. To avoid product overheating, a removed power supply must be replaced within five minutes.

Did fan module (power supply) replacement solve the problem?

NO YES

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

7

A power supply failed POSTs (as indicated by FRU code **06**) and must be removed and replaced. Refer to [RRP 2: Redundant Power Supply](#) on page 5-6.

- This procedure is concurrent and can be performed while switch power is on.
- Perform the data collection procedure as part of FRU removal and replacement.
- If multiple power supply failures occurred, connect the switch to facility AC power after both power supplies are replaced.

ATTENTION ! Do not remove a power supply unless a replacement FRU is immediately available. To avoid product overheating, a removed power supply must be replaced within five minutes.

Did power supply replacement solve the problem?

NO YES

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

8

POST/IPL diagnostics detected a firmware failure (as indicated by event code **411**) and performed an online dump. All Fibre Channel ports reset after the failure and devices momentarily logout, login, and resume operation.

Perform the data collection procedure and return the CD to McDATA for analysis. **Exit MAP.**

MAP 0300: Server Application Problem Determination

This map describes isolation of management server or customer-supplied server application problems, including those associated with the Windows 2000 Professional operating system, SAN management application (SANavigator 4.0 or EFCM 8.0), or Sphereon 4500 Element Manager application.

1

Did the rack-mount management server or customer-supplied server lock up or crash without displaying a warning or error message?

YES NO



Go to [step 4](#).

2

An application or operating system problem is indicated. Close the SAN management application (at the browser-capable PC connected through an Ethernet LAN segment to the management server).

- a. At the management server's Windows 2000 desktop, click the **Send Ctrl-Alt-Del** button at the top of the window. The *Windows Security* dialog box displays ([Figure 3-14](#)).

NOTE: Do not simultaneously press the **Ctrl**, **Alt**, and **Delete** keys. This action controls the browser-capable PC, not the rack-mount server.



Figure 3-14 Windows Security Dialog Box

- b. Click *Task Manager*. The *Windows Task Manager* dialog box displays with the *Applications* page open by default (Figure 3-15).

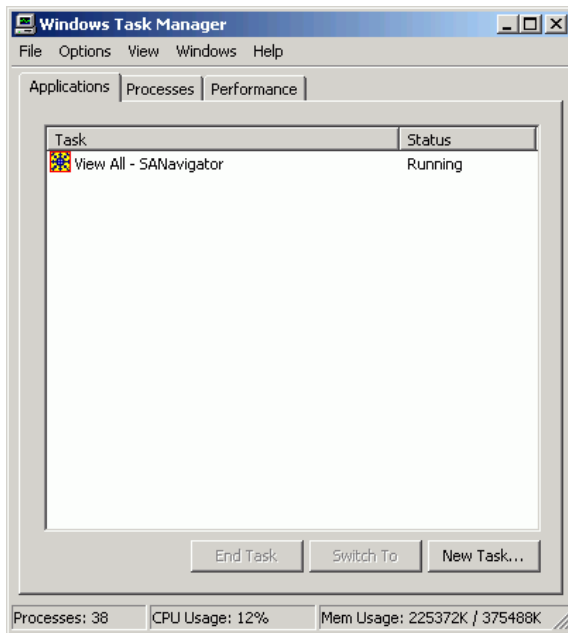


Figure 3-15 Windows Task Manager Dialog Box (Applications Page)

- c. Select (highlight) the *SAnavigator* or *EFCM* entry and click *End Task*. The SAN management application closes.

Continue to the next step.

3

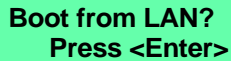
Attempt to clear the problem by rebooting the management server or customer-supplied server PC. If the customer-supplied server does not use the Windows 2000 operating system, refer to the supporting documentation to reboot the server.

- a. At the Windows 2000 desktop, click *Start* at the left side of the task bar (bottom of the desktop), then select *Shut Down*. The *Shut Down Windows* dialog box displays (Figure 3-16 on page 3-43).



Figure 3-16 Shut Down Windows Dialog Box

- b. Select the *Shut Down* option from the list box and click *OK*. The management server powers down.
- c. Wait approximately 30 seconds and press the power (⏻) button on the LCD panel to power on the server and perform POSTs. During POSTs:
 - 1. The green LCD panel illuminates.
 - 2. The green **HDD** LED blinks momentarily, and processor speed and random-access memory information display momentarily at the LCD panel.
 - 3. After a few seconds, the LCD panel displays the following message pertaining to boot sequence selection (Figure 3-17):

A green rectangular box with a black border containing the text "Boot from LAN?" and "Press <Enter>" in black font.

Boot from LAN?
Press <Enter>

Figure 3-17 LCD Panel During Boot Sequence

4. Ignore the message. After ten seconds, the server performs the boot sequence from the BIOS. During the boot sequence, the server performs additional POSTs and displays the following operational information at the LCD panel:
 - Host name.
 - System date and time.
 - LAN 1 and LAN 2 IP addresses.
 - Fan 1, fan 2, fan 3, and fan 4 rotational speed.
 - CPU temperature.
 - Hard disk capacity.
 - Virtual and physical memory capacity.
- d. After successful POST completion, the LCD panel displays a **Welcome!!** message, then continuously cycles through and displays server operational information.
- e. After rebooting the server at the LCD panel, log on to the management server's Windows 2000 desktop through a LAN connection to a browser-capable PC. Refer to [Access the Management Server Desktop](#) on page 2-55 for instructions. The SAN management application starts and the *SANavigator Log In* or *EFCM Log In* dialog box displays ([Figure 3-18](#)).

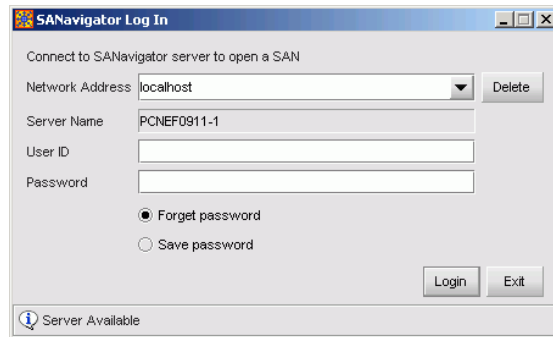


Figure 3-18 SANavigator Login or EFCM Login Dialog Box

- f. Type a user ID and password (obtained in [MAP 0000: Start MAP](#), and both are case sensitive), and click *Login*. The SAN management application opens and the SANavigator or EFCM main window displays ([Figure 3-9](#) on page 3-17).

Did the main window display and does the SAN management application appear operational?

NO YES



The problem is transient and the management server or customer-supplied server appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

4

Did the SAN management application display a dialog box with the message **Connection to management server lost - click OK to exit application** or **SANavigator or EFCM error *n*** (where *n* is an error message number 1 through 8 inclusive)?

NO YES



A SAN management application error occurred. Click *OK* to close the window and close the application. **Go to [step 3](#).**

5

Did the SAN management application display a window with the message **The software version on this management server is not compatible with the version on the remote management server?**

YES NO



Go to [step 8](#).

6

The SAN management applications running on the management server and client workstation are not at compatible release levels. Recommend to the customer that the downlevel version be upgraded.

Does the customer want the SAN management application upgraded?

YES NO

↓ Power off the client workstation. **Exit MAP.**

7

Upgrade the downlevel SAN management application. Refer to [Install or Upgrade Software](#) on page 4-87.

Did the software upgrade solve the problem?

NO YES

↓ The management server or customer-supplied server appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

8

Did the Element Manager application display a window with the message **Element Manager error 5001** or **Element Manager error 5002**?

NO YES

↓ An Element Manager application error occurred. Click *OK* to close the window and close the SAN management and Element Manager applications. **Go to step 3.**

9

Did the Element Manager application display a window with the message **Send firmware failed**?

YES NO

↓ **Go to step 11.**

10

An attempt to download a firmware version from the management server or customer-supplied server hard drive to the switch failed. Retry the operation. Refer to [Manage Firmware Versions](#) on page 4-59.

Did the firmware version download to the switch?

NO **YES**

↓ The management server or customer-supplied server appears operational. **Exit MAP.**

A CTP card failure is suspected. Go to [MAP 0000: Start MAP](#) on page 3-6 to isolate the problem. **Exit MAP.**

11

Did the Element Manager application display a window with the message **The data collection process failed**?

YES **NO**

↓ Go to [step 13](#).

12

The data collection process failed. Retry the process using a new CD. Refer to [Collect Maintenance Data](#) on page 4-44.

Did the data collection process complete?

NO **YES**

↓ **Exit MAP.**

Contact the next level of support. **Exit MAP.**

13

Did the management server or customer-supplied server lock up or crash and display a *Dr. Watson for Windows 2000* dialog box ([Figure 3-19](#))?

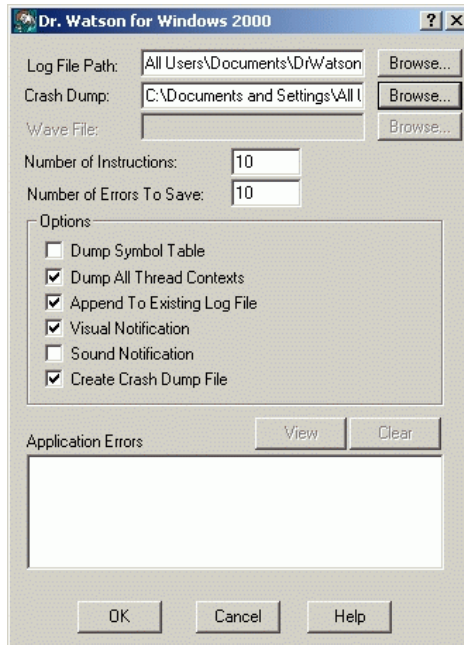


Figure 3-19 Dr. Watson for Windows 2000 Dialog Box

YES NO



Go to [step 14](#).

A SAN management application error occurred and transmitted a handling exception event to the operating system.

- Click *Cancel* to close the *Dr. Watson for Windows 2000* dialog box and SAN management application.
- Using the *My Computer* function at the Windows 2000 desktop, copy the crash dump file (**user.dmp**) from the local disk (**C:**) to the CD-RW drive (**D:**).
- At the management server, press the left edge (**PUSH** label) of the LCD panel to disengage the panel and expose the CD-RW drive.
- Remove the CD and return it to McDATA customer support personnel for analysis.

Go to [step 3](#).

14

Did the management server or customer-supplied server crash and display a blue screen with the system dump file in hexadecimal format (blue screen of death)?

YES NO



The management server or customer-supplied server appears operational. **Exit MAP.**

15

Attempt to clear the problem by power cycling the management server or customer-supplied server PC. If the customer-supplied server does not use the Windows 2000 operating system, refer to the supporting documentation to reboot the server.

- a. At the rack-mount management server, press the power (⏻) button on the LCD panel to power off the server.
- b. Wait approximately 30 seconds and press the power (⏻) button to power on the server and perform POSTs. During POSTs:
 1. The green LCD panel illuminates.
 2. The green **HDD** LED blinks momentarily, and processor speed and random-access memory information display momentarily at the LCD panel.
 3. After a few seconds, the LCD panel displays the following message pertaining to boot sequence selection ([Figure 3-20](#) on page 3-49):

A green rectangular box with a black border containing the text "Boot from LAN?" and "Press <Enter>" in black font.

Boot from LAN?
Press <Enter>

Figure 3-20 LCD Panel During Boot Sequence

4. Ignore the message. After ten seconds, the server performs the boot sequence from BIOS. During the boot sequence, the server performs additional POSTs and displays the following operational information at the LCD panel:
 - Host name.
 - System date and time.
 - LAN 1 and LAN 2 IP addresses.

- Fan 1, fan 2, fan 3, and fan 4 rotational speed.
 - CPU temperature.
 - Hard disk capacity.
 - Virtual and physical memory capacity.
- c. After successful POST completion, the LCD panel displays a **Welcome!!** message, then continuously cycles through and displays server operational information.
- d. After rebooting the server at the LCD panel, log on to the management server's Windows 2000 desktop through a LAN connection to a browser-capable PC. Refer to [Access the Management Server Desktop](#) on page 2-55 for instructions. The SAN management application starts and the *SANavigator Log In* or *EFCM Log In* dialog box displays ([Figure 3-21](#)).

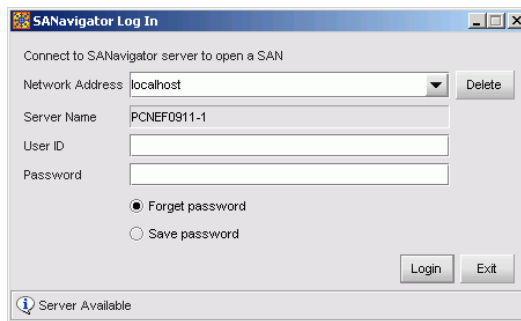


Figure 3-21 SANavigator Login or EFCM Login Dialog Box

- e. Type a user ID and password (obtained in [MAP 0000: Start MAP](#), and both are case sensitive), and click *Login*. The SAN management application opens and the SANavigator or EFCM main window displays ([Figure 3-9](#) on page 3-17).

Did the main window display and does the SAN management application appear operational?

NO YES



The problem is transient and the management server or customer-supplied server appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

MAP 0400: Loss of Server Communication

This MAP describes fault isolation of the Ethernet communication link between a switch and the management server or customer-supplied server, or between a switch and a web browser PC running the SANpilot interface. Failure indicators include:

- Event codes recorded at the SANpilot event log or Sphereon 4500 *Event Log*.
- At the web browser PC, **A Page cannot be found, Unable to locate the server, HTTP 404 - file not found**, or other similar message.
- At the SANavigator or EFCM main window, a grey square with an exclamation mark associated with the icon representing the switch reporting the problem.
- At the *Hardware View*, a grey square at the alert panel, a **No Link** status and reason at the *Sphereon 4500 Status* table, and no FRUs visible for the switch.

When the logical connection between the switch and management server or customer-supplied server is initiated, it may take up to five minutes for the link to activate at the SANavigator or EFCM main window. This delay is normal.

ATTENTION ! Prior to servicing a product, management server, or customer-supplied server, determine the Ethernet LAN configuration. Installation of products and servers on a public customer intranet can complicate problem determination and fault isolation.

1

Is fault isolation being performed at the SANpilot interface?

YES NO



Fault isolation is being performed at the management server or customer-supplied server. **Go to step 7.**

2

Does the SANpilot interface appear operational?

NO YES



The switch-to-SANpilot PC connection is restored and appears operational. **Exit MAP.**

3

A **Page cannot be found, Unable to locate the server, HTTP 404 - file not found**, or other similar message appears. The message indicates the PC cannot communicate with the switch because:

- The switch-to-PC Internet (Ethernet) link could not be established.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP card failed.

Continue to the next step.

4

Ensure the switch is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES NO



A power distribution problem is indicated. Go to [MAP 0100: Power Distribution Analysis](#) on page 3-30. **Exit MAP.**

5

At the front of the switch, inspect the amber **ERR** LED.

Is the LED illuminated?

NO YES



A FRU failure or link incident is indicated. Go to [MAP 0000: Start MAP](#) on page 3-6. **Exit MAP.**

6

Either a switch-to-PC Internet link problem (Internet too busy or IP address typed incorrectly) or a switch Ethernet port failure is indicated.

- a. Wait approximately five minutes, then attempt to login to the switch again.
- b. At the *Netsite* field (Netscape Navigator) or *Address* field (Internet Explorer), type **http://xxx.xxx.xxx.xxx**, where **xxx.xxx.xxx.xxx** is the IP address of the switch (obtained in [MAP 0000: Start MAP](#)). The *Username and Password Required* dialog box appears.
- c. Type the user name and password obtained in [MAP 0000: Start MAP](#) and click **OK**. If the *View* panel does not display, wait five minutes and perform this step again.

Does the SANpilot interface appear operational with the *View* panel displayed?

NO YES

- ↓ The switch-to-SANpilot PC connection is restored and appears operational. **Exit MAP.**

Failure of the switch Ethernet port is indicated. Replace the switch.
Exit MAP.

7

At the SANavigator or EFCM main window's physical map or product list, is a grey square with yellow exclamation mark associated with the icon representing the switch reporting the problem?

YES NO

- ↓ The switch-to-server connection is restored and appears operational. **Exit MAP.**

The status symbol indicates the management server or customer-supplied server cannot communicate with the switch because:

- The switch-to-server Ethernet link failed.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP card failed.

Continue to the next step.

8

Ensure the switch reporting the problem is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES NO

- ↓ A power distribution problem is indicated. Go to [MAP 0100: Power Distribution Analysis](#) on page 3-30. **Exit MAP.**

9

At the front of the switch, inspect the amber **ERR** LED.

Is the LED illuminated?

NO YES

- ↓ A FRU failure or link incident is indicated. Go to [MAP 0000: Start MAP](#) on page 3-6. **Exit MAP.**

10

The switch-to-server Ethernet link failed. At the physical map, right-click the icon with the grey square and exclamation mark representing the switch reporting the problem. A pop-up menu appears. Select the *Element Manager* option from the menu. The Element Manager application opens and the *Hardware View* ([Figure 3-10](#) on page 3-20) displays. At the *Hardware View*:

- A grey square appears at the alert panel.
- No FRUs are visible for the switch.
- The *Sphereon 4500 Status* table is yellow, the *Status* field displays **No Link**, and the **Reason** field displays an error message.

[Table 3-7](#) on page 3-55 lists the error messages and associated steps that describe fault isolation procedures.

Table 3-7 MAP 400 Error Messages

Error Message	Action
Never connected.	Go to step 11 .
Link timeout.	Go to step 11 .
Protocol mismatch.	Go to step 18 .
Duplicate session.	Go to step 21 .
Unknown network address.	Go to step 24 .
Incorrect product type.	Go to step 26 .

11

Transmit or receive errors for a switch's Ethernet adapter exceeded a threshold, the switch-to-server link was not connected, or the switch-to-server link timed out. A problem with the Ethernet cable, Ethernet hub or hubs, or other LAN-attached device is indicated.

Verify the switch is connected to the management server or customer-supplied server through one or more Ethernet hubs.

- Ensure an RJ-45 Ethernet cable connects the switch to an Ethernet hub. If not, connect the cables as directed by the customer.
- Ensure an RJ-45 Ethernet cable connects the management server to an Ethernet hub. If not, connect the cable as directed by the customer.
- Ensure the Ethernet cables are not damaged. If damaged, replace the cables.

Was a corrective action performed?

NO YES

↓ **Go to [step 1](#).**

12

Does the LAN configuration use multiple (up to four) Ethernet hubs that are daisy-chained?

YES NO

↓ **Go to [step 14](#).**

13

Verify the hubs are correctly daisy-chained (Figure 3-22).

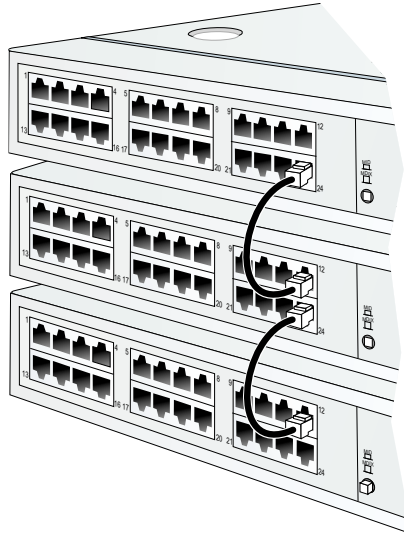


Figure 3-22 Daisy-Chained Ethernet Hubs

- At the first (top) Ethernet hub, ensure an RJ-45 Ethernet patch cable connects to port **24** and the medium-dependent interface (MDI) switch is set to **MDI (in)**.
- At the middle Ethernet hub, ensure the patch cable from the top hub connects to port **12**, the patch cable from the bottom hub connects to port **24**, and the MDI switch is set to **MDI (in)**.
- At the bottom Ethernet hub, ensure the patch cable from the middle hub connects to port **12** and the MDI switch is set to **MDIX (out)**.

NOTE: To check two hubs, use [step b](#) and [step c](#) (middle and bottom hub instructions only).

Was a corrective action performed?

NO **YES**



Go to [step 1](#).

14

Verify operation of the Ethernet hub or hubs. Inspect each hub for indications of being powered on, such as:

- Green **Power** LED illuminated.
- Green **Status** LEDs illuminated.

Is a hub failure indicated?

YES **NO**



Go to [step 16](#).

15

Remove and replace the Ethernet hub. Refer to the supporting documentation shipped with the hub for instructions.

Did hub replacement solve the problem?

NO **YES**



The switch-to-server connection is restored and appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

16

A problem with another LAN-attached device is indicated.

- If the problem is associated with another switch, management server, or customer-supplied server, go to [MAP 0000: Start MAP](#) on page 3-6 to isolate the problem for that device. **Exit MAP.**
- If the problem is associated with an unrelated device, notify the customer and have the system administrator correct the problem.

Did repair of an unrelated LAN-attached device solve the problem?

NO **YES**



The switch-to-server connection is restored and appears operational. **Exit MAP.**

17

The Ethernet adapter on the switch CTP card reset in response to an error. The connection to the management server or customer-supplied server terminated briefly, then recovered upon reset.

Perform the data collection procedure and return the CD to McDATA for analysis. **Exit MAP.**

18

A protocol mismatch occurred because the SAN management application and the switch firmware are not at compatible release levels. Recommend to the customer that the downlevel version (software or firmware) be upgraded.

Does the SAN management application require upgrade?

YES NO

↓ **Go to [step 20](#).**

19

Upgrade the SAN management application. Refer to [Install or Upgrade Software](#) on page 4-87.

Did the switch-to-server Ethernet connection recover?

NO YES

↓ The switch-to-server connection is restored and appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

20

A switch firmware upgrade is required. Refer to [Manage Firmware Versions](#) on page 4-59. Perform the data collection procedure after the upgrade.

Did the switch-to-server Ethernet connection recover?

NO YES

↓ The switch-to-server connection is restored and appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

21

An instance of the SAN management application is open at another management server or customer-supplied server and is communicating with the switch (duplicate session). Notify the customer and either:

- Power off the management server or customer-supplied server running the second instance of the application, or
- Configure the management server or customer-supplied server running the second instance of the application as a client workstation.

Does the customer want the second management server or customer-supplied server configured as a client?

YES NO



Power off the management server or customer-supplied server reporting the **Duplicate Session** communication problem. **Exit MAP.**

22

Determine the internet protocol (IP) address of the management server or customer-supplied server running the first instance of the SAN management application.

- a. After the management server powers on and successfully completes POSTs, the LCD panel displays a **Welcome!!** message, then continuously cycles through and displays the following operational information:
 - Host name.
 - System date and time.
 - LAN 1 and LAN 2 IP addresses.
 - Fan 1, fan 2, fan 3, and fan 4 rotational speed.
 - CPU temperature.
 - Hard disk capacity.
 - Virtual and physical memory capacity.

- b. After a few seconds, the LCD panel displays the following (Figure 3-23):

A green rectangular LCD panel with a black border. It displays the text "LAN 2:" on the first line and "010.001.001.001" on the second line in black, sans-serif font.

LAN 2:
010.001.001.001

Figure 3-23 LCD Panel (LAN 2 IP Address)

- c. Depending on switch-to-server LAN connectivity, record the appropriate IP address (LAN 1 or LAN 2).

Continue to the next step.

23

Configure the management server or customer-supplied server reporting the **Duplicate Session** communication problem as a client.

- At the SANavigator or EFCM main window, select *Logout* from the *SAN* menu. The application logs out and the *SANavigator Log In* or *EFCM Log In* dialog box displays (Figure 3-21 on page 3-50).
- Type a user ID and password (obtained in *MAP 0000: Start MAP*, and both are case sensitive).
- Type the IP address of the management server or customer-supplied server running the first instance of the SAN management application in the *Network Address* field.
- Click *Login*. The SAN management application opens and the SANavigator or EFCM main window displays (Figure 3-9 on page 3-17).

Did the management server or customer-supplied server reconfigure as a client and did the Ethernet connection recover?

NO YES

- ↓ The switch-to-server connection is restored and the second management server or customer-supplied server appears operational as a client. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

24

The IP address defining the switch to the SAN management application is incorrect or unknown and must be verified. A maintenance terminal (PC) and asynchronous RS-232 null modem cable are required to verify the switch IP address. The tools are provided with the switch or by service personnel. To verify the IP address:

- a. Remove the protective cap from the 9-pin maintenance port at the rear of the switch (a phillips screwdriver may be required). Connect one end of the RS-232 null modem cable to the port.
- b. Connect the other cable end to a 9-pin communication port (**COM1** or **COM2**) at the rear of the maintenance terminal PC.
- c. Power on the maintenance terminal. After the PC powers on, the Windows desktop displays.
- d. At the Windows desktop, click *Start* at the left side of the task bar. The *Windows Workstation* menu displays.

NOTE: The following steps describe inspecting the IP address using HyperTerminal serial communication software.

- e. At the *Windows Workstation* menu, sequentially select *Programs*, *Accessories*, *Communications*, and *HyperTerminal*. The *Connection Description* dialog box displays (Figure 3-24).



Figure 3-24 Connection Description Dialog Box

- f. Type **Sphereon 4500** in the *Name* field and click *OK*. The *Connect To* dialog box displays (Figure 3-25).

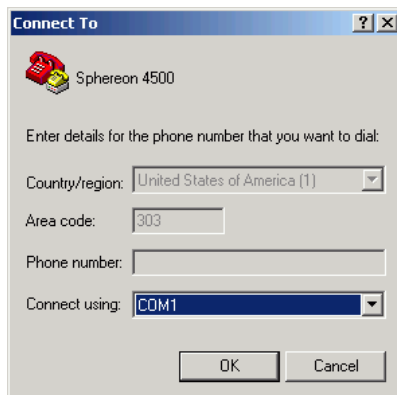


Figure 3-25 Connect To Dialog Box

- g. Ensure the *Connect using* field displays **COM1** or **COM2** (depending on the serial communication port connection to the switch), and click *OK*. The *COMn* dialog box displays, where *n* is 1 or 2 (Figure 3-26).

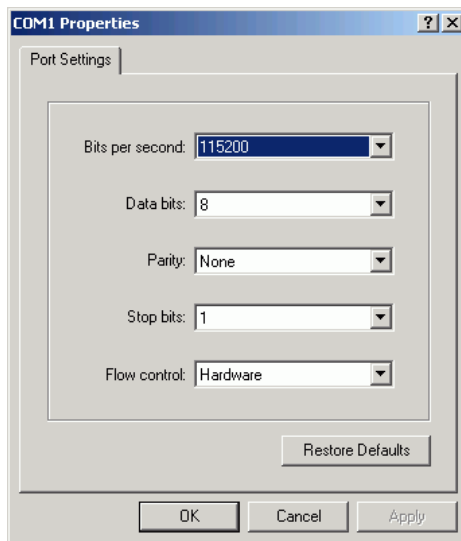


Figure 3-26 COMn Properties Dialog Box

h. Configure the *Port Settings* parameters as follows:

- *Bits per second* - **115200**.
- *Data bits* - **8**.
- *Parity* - **None**.
- *Stop bits* - **1**.
- *Flow control* - **Hardware** or **None**.

When the parameters are set, click *OK*. The *Sphereon 4500 - HyperTerminal* dialog box displays.

- i. At the **>** prompt, type the user-level password (default is **password**) and press **Enter**. The password is case sensitive. The *Sphereon 4500 - HyperTerminal* dialog box displays with a **C>** prompt at the bottom of the window.
- j. At the **C>** prompt, type **ipconfig** and press **Enter**. The *Sphereon 4500 - HyperTerminal* dialog box displays with configuration information listed, including the IP address (Figure 3-27).

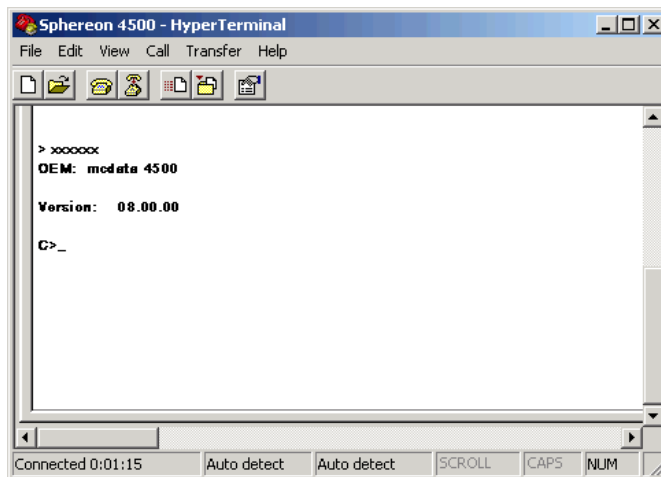


Figure 3-27 Sphereon 4500 - HyperTerminal Dialog Box

- k. Record the switch IP address.
- l. Select *Exit* from the *File* pull-down menu to close the HyperTerminal application. A *HyperTerminal* dialog box displays (Figure 3-28 on page 3-64).

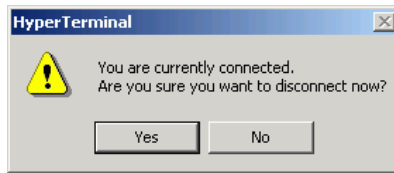


Figure 3-28 HyperTerminal Dialog Box

- m. Click *Yes*. A second *HyperTerminal* dialog box displays ([Figure 3-29](#)).

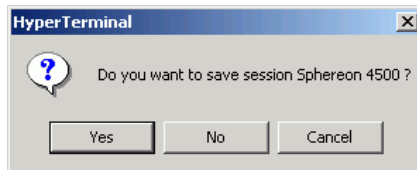


Figure 3-29 HyperTerminal Dialog Box

- n. Click *No* to exit and close the HyperTerminal application.
- o. Power off the maintenance terminal.
- p. Disconnect the RS-232 null modem cable from the switch and the maintenance terminal. Replace the protective cap over the maintenance port.

Continue to the next step.

25

Define the switch's correct IP address (determined in [step 24](#)) to the management server or customer-supplied server.

- a. At the SAN management application (SANavigator or EFCM main window), select the *Setup* option from the *Discover* menu. The *Discover Setup* dialog box displays ([Figure 3-30](#) on page 3-65).

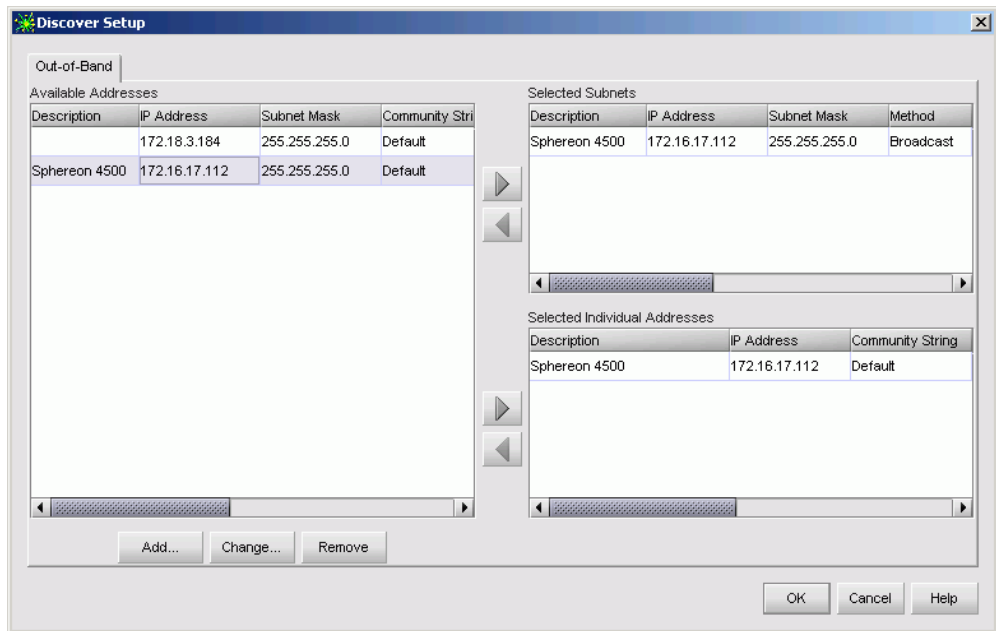


Figure 3-30 Discover Setup Dialog Box

- b. At the *Available Addresses* field, select (highlight) the switch to be reconfigured and click *Change*. The *Editing Domain Information* dialog box displays (Figure 3-31).

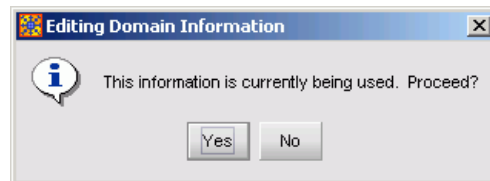


Figure 3-31 Editing Domain Information Dialog Box

- c. Click *Yes*. The *Domain Information* dialog box displays with the *IP Address* page open by default (Figure 3-32 on page 3-66).

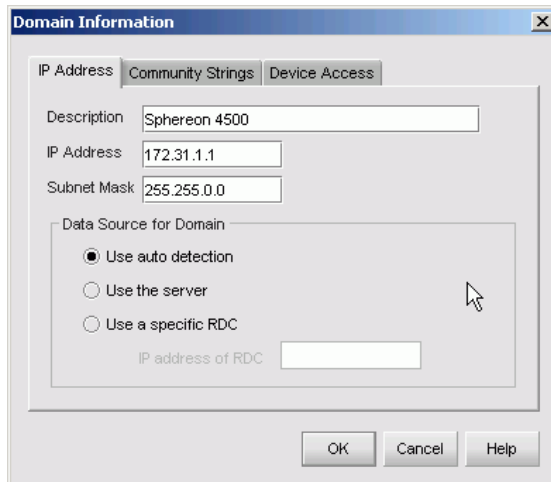


Figure 3-32 Domain Information Dialog Box (IP Address Page)

- d. Type the correct switch IP address in the *IP Address* field.
- e. Click *OK* to save the new IP address, close the dialog box, and redefine the switch to the SAN management application.
- f. Click *OK* to close the *Discover Setup* dialog box and return to the SAN management application.

At the SAN management application master log, did the IP address associated with the switch change to the new entry and did the Ethernet connection recover?

NO YES



The switch-to-server connection is restored and appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

26

An incorrect product type is defined to the management server or customer-supplied server.

- a. Right-click the product icon with a grey square and yellow exclamation mark (representing the switch reporting the problem) at the SAN management application's physical map. A pop-up menu appears.

- b. Select the *Delete* option from the pop-up menu. The *SANavigator* or *EFCM Message* dialog box displays (Figure 3-33).

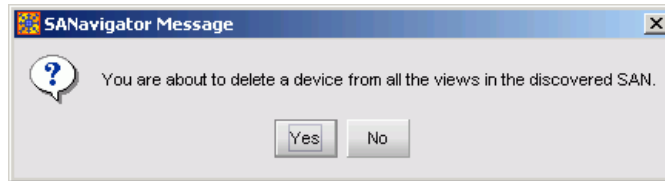


Figure 3-33 SANavigator or EFCM Message Dialog Box

- c. Click *Yes* to delete the switch.
- d. At the SAN management application main window, select the *Setup* option from the *Discover* menu. The *Discover Setup* dialog box displays (Figure 3-30 on page 3-65).
- e. Click *Add*. The *Domain Information* dialog box displays with the *IP Address* page open by default (Figure 3-34).

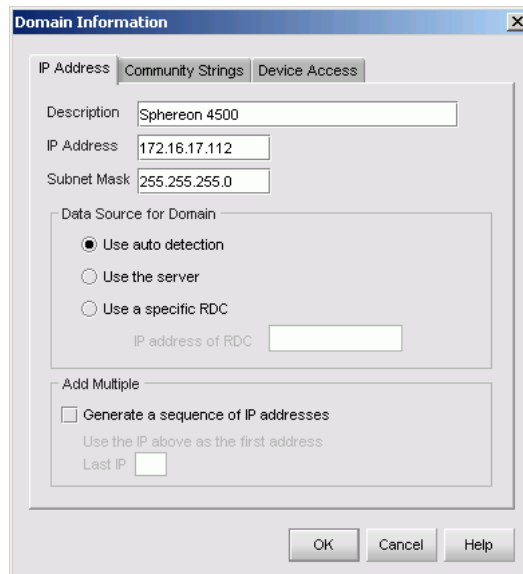


Figure 3-34 Domain Information Dialog Box (IP Address Page)

- f. Type a switch description in the *Description* field.
- g. Type the switch IP address (determined by the customer's network administrator) in the *IP Address* field.
- h. Type the switch subnet mask (determined by the customer's network administrator) in the *Subnet Mask* field.
- i. At the *Data Source for Domain* area of the dialog box, select the *Use auto detection*, *Use the server*, or *Use a specific RDC* radio button (determined by the customer's network administrator).
- j. Click *OK* to save the entered information, close the dialog box, and define the new product configuration to the SAN management application.
- k. Click *OK* to close the *Discover Setup* dialog box and return to the SAN management application.

At the SAN management application master log, did the IP address associated with the switch change to the new product configuration and did the Ethernet connection recover?

NO YES

↓ The switch-to-server connection is restored and appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

MAP 0500: FRU Failure Analysis

This MAP describes fault isolation for the switch and FRUs. Failure indicators include:

- An event code recorded at the SANpilot event log or Sphereon 4500 *Event Log* (management server).
- The amber LED on the FRU illuminates.
- A **Failed** message associated with a FRU at the SANpilot interface.
- The amber emulated LED on a power supply at the *Hardware View* illuminates.
- A blinking red and yellow diamond (failed FRU indicator) appears over a FRU graphic; or a grey square (status unknown indicator) or yellow triangle (attention indicator) appears at the alert panel of the *Hardware View*.

1

Was an event code **300, 301, 302, 303, 304, 305, 426, 433, 440, 810,** or **811** observed at the SANpilot event log or at the Spheron 4500 *Event Log*?

YES NO



Go to [step 3](#).

2

[Table 3-8](#) lists event codes, brief explanations of the codes, and associated steps that describe fault isolation procedures.

Table 3-8 MAP 500 Event Codes

Event Code	Explanation	Action
300	Cooling fan propeller failed.	Go to step 6 .
301	Cooling fan propeller failed.	Go to step 6 .
302	Cooling fan propeller failed.	Go to step 6 .
303	Cooling fan propeller failed.	Go to step 6 .
304	Cooling fan propeller failed.	Go to step 6 .
305	Cooling fan propeller failed.	Go to step 6 .
426	Multiple ECC single-bit errors occurred.	Go to step 9 .
433	Non-recoverable Ethernet fault.	Go to step 10 .
440	Embedded port hardware failed.	Go to step 10 .
810	High temperature warning (CTP thermal sensor).	Go to step 9 .
811	Critically hot temperature warning (CTP thermal sensor).	Go to step 9 .

3

Is fault isolation being performed at the switch?

YES NO



Fault isolation is being performed at the SANpilot interface, management server, or customer-supplied server. **Go to [step 11](#).**

4

Ensure the switch reporting the problem is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES NO

- ↓ Both power supply modules failed or the CTP card failed. Go to [MAP 0000: Start MAP on page 3-6](#). If this is the second time at this step and a dual power supply failure is ruled out, a CTP card failure is indicated. Replace the switch. **Exit MAP.**

5

Inspect both power supply modules (with internal switch cooling fans) at the rear of the switch.

Does inspection of a power supply and fan module (combined FRU) indicate a failure? Indicators include:

- The amber LED is illuminated on one or both power supplies.
- One or more cooling fans are not rotating.

YES NO

- ↓ **Go to [step 7](#).**

6

Visual inspection or an event code **300, 301, 302, 303, 304, or 305** indicates one or more cooling fans failed, and one or both power supplies (combined FRUs) must be removed and replaced. Refer to [RRP 2: Redundant Power Supply](#) on page 5-6.

- This procedure is concurrent and can be performed while switch power is on.
- If multiple fan failures caused a thermal shutdown, connect the switch to facility AC power after the power supply(s) are replaced.

- Perform the data collection procedure as part of FRU removal and replacement.

ATTENTION ! Do not remove a power supply unless a replacement FRU is immediately available. To avoid product overheating, a removed power supply must be replaced within five minutes.

Do the fan and power supply module(s) appear to function?

NO YES

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

7

Inspect the switch front panel.

Is the green **PWR** LED illuminated and the amber **ERR** LED illuminated and blinking (beaconing)?

YES NO

↓ **Go to step 8.**

Beaconing is enabled for the switch.

- a. Consult the customer and next level of support to determine the reason switch (unit) beaconing is enabled.
- b. Disable unit beaconing.
 1. At the *Hardware View* ([Figure 3-10](#) on page 3-20), right-click the front bezel graphic (away from a FRU). A pop-up menu appears.
 2. Click the *Enable Unit Beaconing* option. The check mark disappears from the box adjacent to the option, and unit beaconing is disabled.

Was switch beaconing enabled because a FRU failure or degradation was suspected?

NO YES

↓ **Go to step 1.**

The switch appears operational. **Exit MAP.**

8

Is the green **PWR** LED illuminated, the amber **ERR** LED illuminated, and all Fibre Channel traffic disrupted (not operational)?

NO **YES**

↓ A CTP card failure is indicated. Replace the switch.
Exit MAP.

Analysis for this failure is not described in this MAP. Go to [MAP 0000: Start MAP](#) on page 3-6. If this is the second time at this step, contact the next level of support. **Exit MAP.**

9

An event code **426** (SDRAM problem), **810** (high-temperature warning), or **811** (critically-hot temperature warning) indicates an intermittent problem that may result in switch failure.

Is the appearance of this event code a recurring problem?

NO **YES**

↓ A CTP card failure is indicated. Replace the switch.
Exit MAP.

Perform the data collection procedure and contact the next level of support. Refer to [Collect Maintenance Data](#) on page 4-44. **Exit MAP.**

10

An event code **433** or **440** indicates a CTP card failure. Replace the switch. **Exit MAP.**

11

Is fault isolation being performed at the SANpilot interface?

YES **NO**

↓ Fault isolation is being performed at the management server or customer-supplied server. **Go to step 16.**

12

Does the SANpilot interface appear operational?

NO **YES**

↓ **Go to step 14.**

13

A **Page cannot be found, Unable to locate the server, HTTP 404 - file not found**, or other similar message appears. The message indicates the PC cannot communicate with the switch because:

- The switch-to-PC Internet link could not be established.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP card failed.

The SANpilot interface is not operational and fault isolation must be performed at the switch or management server. **Go to step 1.** If this is the second time at this step, contact the next level of support. **Exit MAP.**

14

Inspect fan module operational states at the SANpilot interface.

- a. At the *View* panel, click the *FRU Properties* tab. The *View* panel (*FRU Properties* tab) displays.
- b. Inspect the *Status* fields for both power supplies.

Does the *Status* field display a **Failed** message for either fan module?

NO **YES**



A fan module failure is indicated. **Go to step 6.**

15

Inspect switch CTP operational states at the SANpilot interface. Inspect the *Status* fields for the switch CTP.

Does the *Status* field display a **Failed** message for the CTP?

NO **YES**



A CTP card failure is indicated. Replace the switch.
Exit MAP.

Additional analysis is not described in this MAP. Go to [MAP 0000: Start MAP](#) on page 3-6. If this is the second time at this step, contact the next level of support. **Exit MAP.**

16

Does a blinking red and yellow diamond (failed FRU indicator) appear to overlay a combined fan module and power supply graphic at the *Hardware View* ([Figure 3-10](#) on page 3-20)?

NO YES



A fan module failure is indicated. **Go to [step 6](#).**

17

At the *Hardware View*, does a grey square appear at the alert panel, a **No Link** status appear at the *Sphereon 4500 Status* table, and graphical FRUs appear uninstalled?

YES NO



A green circle appears at the alert panel and the switch appears operational. **Exit MAP.**

The grey square indicates the management server or customer-supplied server cannot communicate with the switch because:

- The switch-to-server Ethernet link failed.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP card failed.

Go to [MAP 0000: Start MAP](#) on page 3-6. If this is the second time at this step and an Ethernet link or AC power distribution failure is ruled out, a CTP card failure is indicated. Replace the switch. **Exit MAP.**

MAP 0600: Port Failure and Link Incident Analysis

This MAP describes fault isolation for shortwave laser small form factor pluggable (SFP) optical transceivers, longwave laser SFP optical transceivers, and Fibre Channel link incidents. Failure indicators include:

- An event code recorded at the SANpilot event log or Sphereon 4500 *Event Log* (management server).
- A link incident event code recorded at the console of an OSI server attached to the switch reporting the problem.
- One or more amber LEDs on the ports illuminate.
- A port operational state message or a **Failed** message associated with a port at the SANpilot interface.
- One or more emulated amber LEDs on a port graphic at the *Hardware View* illuminate.

- A blinking red and yellow diamond (failed FRU indicator) appears over a port graphic or a yellow triangle (attention indicator) appears at the alert panel of the *Hardware View*.
- A link incident message recorded in the *Link Incident Log* or *Port Properties* dialog box.

1

Was an event code **080**, **081**, **506**, **507**, **512**, or **514** observed at the SANpilot event log or at the Sphereon 4500 *Event Log* (management server)?

NO **YES**



Go to [step 3](#).

2

Was an event code **581**, **582**, **583**, **584**, **585**, or **586** observed at the console of an OSI server attached to the switch reporting the problem?

YES **NO**



Go to [step 4](#).

3

[Table 3-9](#) lists event codes, brief explanations of the codes, and associated steps that describe fault isolation procedures.

Table 3-9 MAP 600 Event Codes

Event Code	Explanation	Action
080	Unauthorized worldwide name.	Go to step 21 .
081	Invalid attachment.	Go to step 22 .
506	Fibre Channel port failure.	Go to step 6 .
507	Loopback diagnostics port failure.	Go to step 18 .
512	SFP optical transceiver nonfatal error.	Go to step 6 .
514	SFP optical transceiver failure.	Go to step 6 .
581	Implicit incident.	Go to step 34 .
582	Bit error threshold exceeded.	Go to step 34 .

Table 3-9 MAP 600 Event Codes (Continued)

Event Code	Explanation	Action
583	Loss of signal or loss of synchronization.	Go to step 34 .
584	Not operational primitive sequence received.	Go to step 34 .
585	Primitive sequence timeout.	Go to step 34 .
586	Invalid primitive sequence received for current link state.	Go to step 34 .

4

Is fault isolation being performed at the switch?

YES NO



Fault isolation is being performed at the SANpilot interface, management server, or customer-supplied server. **Go to [step 7](#).**

5

Each port has an amber LED and a blue (2 Gbps operation) or green (1 Gbps operation) LED adjacent to the port. The amber LED illuminates and the blue or green LED extinguishes if the port fails.

Is an amber port LED illuminated but not blinking (beaconing)?

YES NO



The switch appears operational, however a link incident or other problem may have occurred. Perform fault isolation at the management server or customer-supplied server. **Go to [step 13](#).**

6

As indicated by a message or event code **506**, **512**, or **514**, a Fibre Channel port failed and the SFP optical transceiver must be removed and replaced. Refer to [RRP 1: SFP Optical Transceiver](#) on page 5-2.

- This procedure is concurrent and can be performed while the switch is powered on and operational.
- Verify location of the failed port.
- Replace the optical transceiver with a transceiver of the same type (shortwave or longwave).

- Perform an external loopback test for the port as part of FRU removal and replacement. Refer to [Perform Port Diagnostic Loopback Tests](#) on page 4-38.

NOTE: An event code 514 may generate a call-home event that incorrectly indicates a CTP card failure. Although the optical socket may have failed, first replace the optical transceiver and verify operation. If a failure is still indicated, replace the switch. When an even code 514 is indicated, ensure a replacement optical transceiver and a replacement switch are available.

Did optical transceiver replacement solve the problem?

NO YES

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

7

Is fault isolation being performed at the SANpilot interface?

YES NO

↓ Fault isolation is being performed at the management server or customer-supplied server. **Go to step 13.**

8

Does the SANpilot interface appear operational?

NO YES

↓ **Go to step 11.**

9

A **Page cannot be found, Unable to locate the server, HTTP 404 - file not found**, or other similar message appears. The message indicates the PC cannot communicate with the switch because:

- The switch-to-PC Internet link could not be established.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP card failed.

Continue to the next step.

10

Ensure the switch is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES NO



Analysis for an Ethernet link, AC power distribution, or CTP failure is not described in this MAP. Go to [MAP 0000: Start MAP on page 3-6](#). If this is the second time at this step, contact the next level of support. **Exit MAP.**

11

Inspect Fibre Channel port operational states at the SANpilot interface.

- At the *View* panel, click the *Port Properties* tab. The *View* panel (*Port Properties* tab) displays with port **0** highlighted in red.
- Click the port number (**0** through **(23)**) for which a failure is suspected to display properties for that port.
- Inspect the *Operational State* field. Scroll down the *View* panel as necessary.
- [Table 3-10](#) on page 3-78 lists port operational states and MAP 0600 steps that describe fault isolation procedures.

Table 3-10 Port Operational States and Actions (SANpilot)

Operational State	Action
Offline	Go to step 19 .
Not Operational	Go to step 19 .
Port Failure	Go to step 6 .
Testing	Internal or external loopback test in process. Exit MAP.
Invalid Attachment	Go to step 22 .
Link Reset	Go to step 33 .
Not Installed	Go to step 12 .

12

Install an SFP optical transceiver in the port receptacle. Refer to [RRP 1: SFP Optical Transceiver](#) on page 5-2.

- This procedure is concurrent and can be performed while the switch is powered on and operational.
- Verify location of the failed port.
- Perform an external loopback test for the port as part of FRU removal and replacement. Refer to [Perform Port Diagnostic Loopback Tests](#) on page 4-38.

Exit MAP.

13

At the management server, does a blinking red and yellow diamond (failed FRU indicator) appear adjacent to a Fibre Channel port graphic at the *Hardware View* ([Figure 3-10](#) on page 3-20)?

NO YES



A port failure is indicated. **Go to step 6.**

14

Did a Fibre Channel port fail a loopback test?

NO YES



Go to step 18.

15

Does a yellow triangle (attention indicator) appear adjacent to a port graphic at the *Hardware View*?

YES NO



Go to step 17.

16

Inspect the port state and LED status for all ports with an attention indicator.

- a. At the *Hardware View* ([Figure 3-10](#) on page 3-20), double-click the port graphic with the attention indicator. The *Port Properties* dialog box displays.
- b. Inspect the *Operational State* field at the *Port Properties* dialog box, and the emulated green and amber LEDs adjacent to the port at the *Hardware View*.

- c. [Table 3-11](#) lists LED and port operational state combinations and associated MAP 0600 (or other) steps that describe fault isolation procedures.

Table 3-11 Port Operational and LED States (Management Server)

Operational State	Green LED	Amber LED	Action
Offline	Off	Off	Go to step 19 .
Not Operational	Off	Off	Go to step 19 .
Testing	Off	Blinking	Internal loopback test in process. Exit MAP.
Testing	On	Blinking	External loopback test in process. Exit MAP.
Beaconing	Off or On	Blinking	Go to step 20 .
Invalid Attachment	On	Off	Go to step 22 .
Link Reset	Off	Off	Go to step 33 .
Link Incident	Off	Off	Go to step 34 .
Segmented E_Port	On	Off	Go to MAP 0700 .

17

A link incident may have occurred, but the LIN alerts option is not enabled for the port and the attention indicator does not appear.

At the *Hardware View* ([Figure 3-10](#) on page 3-20), click *Logs* and select *Link Incident Log*. The *Link Incident Log* displays. If a link incident occurred, the affected port number is listed with one of the following messages.

Link interface incident - implicit incident.

Link interface incident - bit-error threshold exceeded.

Link failure - loss of signal or loss of synchronization.

Link failure - not-operational primitive sequence (NOS) received.

Link failure - primitive sequence timeout.

Link failure - invalid primitive sequence received for the current link state.

Did one of the listed messages appear in the *Link Incident Log*?

YES NO

↓ The switch appears operational. **Exit MAP.**

Go to [step 34](#).

18

As indicated by a message or event code **507**, a Fibre Channel port failed an internal or external loopback test.

- a. Reset each port that failed the loopback test.
 1. At the *Hardware View* ([Figure 3-10](#) on page 3-20), right-click the port. A pop-up menu appears.
 2. Select *Reset Port*. A **This operation will cause a link reset to be sent to the attached device** message displays.
 3. Click *OK*. The port resets.
- b. Perform an external loopback test for all ports that were reset. Refer to [Perform Port Diagnostic Loopback Tests](#) on page 4-38.

Did resetting ports solve the problem?

NO YES

↓ The switch appears operational. **Exit MAP.**

19

A switch port is unblocked and receiving the offline sequence (OLS) or not operational sequence (NOS) from an attached device.

Inform the customer that the attached device failed or is set offline, and to take the appropriate corrective action. **Exit MAP.**

20

Beaconing is enabled for the port.

- a. Consult the customer and next level of support to determine the reason port beaconing is enabled.
- b. Disable port beaconing.
 1. At the *Hardware View* ([Figure 3-10](#) on page 3-20), right-click the port graphic. A pop-up menu appears.
 2. Click the *Enable Beaconing* option. The check mark disappears from the box adjacent to the option, and port beaconing is disabled.

Was port beaconing enabled because port failure or degradation was suspected?

YES NO

↓ The switch appears operational. **Exit MAP.**

Go to [step 1](#).

21

As indicated by a message or event code **080**, the eight-byte (16-digit) worldwide name (WWN) entered to configure port binding is not valid or a nickname was used that is not configured for the attached device in the Element Manager application.

From the *Hardware View* ([Figure 3-10](#) on page 3-20), click *Node List*. Note the *Port WWN* column. This is the WWN assigned to the port or Fibre Channel interface installed on the attached device.

- If a nickname is not assigned to the WWN, the WWN is prefixed by the device manufacturer's name.
- If a nickname is assigned to the WWN, the nickname appears in place of the WWN.

The bound WWN must be entered in the form of a raw WWN format (**XX:XX:XX:XX:XX:XX:XX:XX**) or must be a valid nickname. Ensure a valid WWN or nickname is entered.

Did configuring the WWN or nickname solve the problem?

NO YES

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

22

As indicated by a message or event code **081**, a port has an invalid attachment. The information in the *Port Properties* dialog box specifies the reason as listed in [Table 3-12](#).

Table 3-12 Invalid Attachment Reasons and Actions

Reason	Action
Unknown	Contact the next level of support.
ISL connection not allowed.	Go to step 23 .
Incompatible switch.	Go to step 24 .

Table 3-12 Invalid Attachment Reasons and Actions (Continued)

Reason	Action
External loopback plug connected.	Go to step 25 .
N-Port connection not allowed.	Go to step 23 .
Non-McDATA switch at other end.	Go to step 24 .
Unauthorized port binding WWN.	Go to step 21 .
Unresponsive node.	Go to step 27 .
ESA security mismatch.	Go to step 29 .
Fabric binding mismatch.	Go to step 30 .
Authorization failure reject.	Go to step 27 .
Unauthorized switch binding WWN.	Go to step 31 .
Fabric mode mismatch.	Go to step 24 .
CNT WAN extension mode mismatch.	Go to step 32 .

23

The port connection conflicts with the configured port type and an ISL connection is not allowed. Either an expansion port (E_Port) is incorrectly cabled to a Fibre Channel device or a fabric port (F_Port) is incorrectly cabled to a fabric element.

- At the management server's *Hardware View* ([Figure 3-10](#) on page 3-20), click *Configure* and select *Ports*. The *Configure Ports* dialog box displays.
- Use the vertical scroll bar as necessary to display the information row for the port indicating an invalid attachment.
- Select (click) the *Type* field and configure the port from the list box as follows:
 - Select fabric port (**F_Port**) if the port is cabled to a device (node).
 - Select expansion port (**E_Port**) if the port is cabled to a fabric element (director or switch) to form an ISL.
- Click *Activate* to save the configuration information and close the window.

Did reconfiguring the port type solve the problem?

NO YES

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

24



One of the following mode-mismatch conditions was detected and an ISL connection is not allowed:

- The switch is configured for operation in **Open Fabric 1.0** mode and is connected to a fabric element not configured to **Open Fabric 1.0** mode.
- The switch is configured for operation in **Open Fabric 1.0** mode and is connected to a legacy McDATA switch at the incorrect Exchange Link Parameter (ELP) revision level.
- The switch is configured for operation in **Open Fabric 1.0** mode and is connected to a non-McDATA switch at the incorrect ELP revision level.
- The switch is configured for operation in **McDATA Fabric 1.0** mode and is connected to a non-McDATA switch.

Reconfigure the switch operating mode:

- a. Ensure the switch is set offline. Refer to [Set the Switch Online or Offline](#) on page 4-48.
- b. At the *Hardware View* ([Figure 3-10](#) on page 3-20), click *Configure* and select *Operating Parameters* and *Fabric Parameters*. The *Configure Fabric Parameters* dialog box displays ([Figure 3-35](#)).

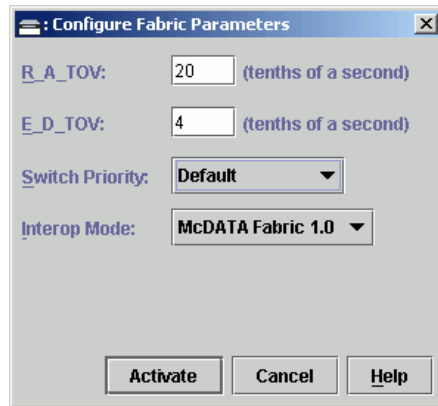


Figure 3-35 Configure Fabric Parameters Dialog Box

- c. Select **McDATA Fabric 1.0** or **Open Fabric 1.0** from the *Interop Mode* list box.
 - Select the **McDATA Fabric 1.0** option if the switch is fabric-attached *only* to other McDATA directors or switches that are also operating in **McDATA Fabric 1.0** mode.
 - Select the **Open Fabric 1.0** option if the switch is fabric-attached to directors or switches produced by other original equipment manufacturers (OEMs) that are open-fabric compliant.
- d. Click *Activate* to save the selection and close the window.

Did configuring the operating mode solve the problem?

NO **YES**

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

25

A loopback (wrap) plug appears to be connected to the port and there is no diagnostic test running. Is a loopback plug in the port receptacle?

YES **NO**

↓ Contact the next level of support. **Exit MAP.**

26

Remove the loopback plug from the port receptacle. If directed by the customer, connect a fiber-optic jumper cable attaching a device to the switch.

- If the port is operational and a device is not attached, both LEDs adjacent to the port extinguish and the port state is *No Light*.
- If the port is operational and a device is attached, the blue or green LED illuminates, the amber LED extinguishes, and the port state is *Online*.

Did removing the loopback plug solve the problem?

NO YES

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

27

A port connection timed out because of an unresponsive device (node) or an ISL connection was not allowed because of a security violation (authorization failure reject). Check the port status and clean the fiber-optic connectors on the cable.

- a. Notify the customer the port will be blocked. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port and sets the attached device offline.
- b. Block the port. Refer to [Block or Unblock a Port](#) on page 4-51.
- c. Disconnect both ends of the fiber-optic cable.
- d. Clean the fiber-optic connectors. Refer to [Clean Fiber-Optic Components](#) on page 4-54.
- e. Reconnect the fiber-optic cable.
- f. Unblock the port. Refer to [Block or Unblock a Port](#) on page 4-51.
- g. Monitor port operation for approximately five minutes.

Is the invalid attachment problem solved?

YES NO

↓ The Fibre Channel link and switch appear operational.
Exit MAP.

28

Inspect and service the host bus adapters (HBAs) as necessary.

Did service of the HBAs solve the problem?

NO YES

↓ **Exit MAP.**

Contact the next level of support. **Exit MAP.**

29

A port connection is not allowed because of an Exchange Security Attribute (ESA) feature mismatch. Switch binding parameters must be compatible for both fabric elements.

- a. At the *Hardware View* ([Figure 3-10](#) on page 3-20) for each switch, click *Configure* and select *Switch Binding* and *Change State*. The *Switch Binding - State Change* dialog box displays ([Figure 3-36](#)).

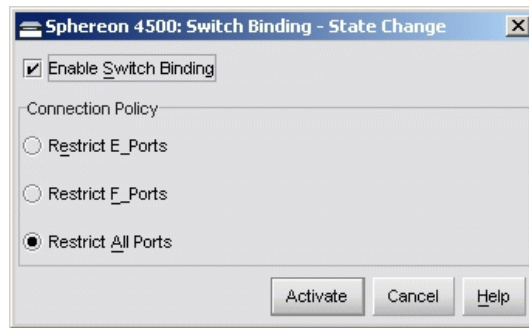


Figure 3-36 Switch Binding - State Change Dialog Box

- b. Ensure the *Enable Switch Binding* checkbox is enabled (checked) for both switches.

- c. Ensure the *Connection Policy* radio buttons are compatible for both switches.
- d. Click *Activate* for each switch. The switch binding feature is consistently enabled for both switches.

Did configuring the switch binding parameters solve the problem?

NO YES

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

30

A port connection is not allowed because of a fabric binding mismatch. Fabric membership lists must be compatible for both fabric elements.

- a. At the SANavigator or EFCM main window, select *Fabric Binding* from the *Configure* menu. The *Fabric Binding* dialog box displays (Figure 3-37).

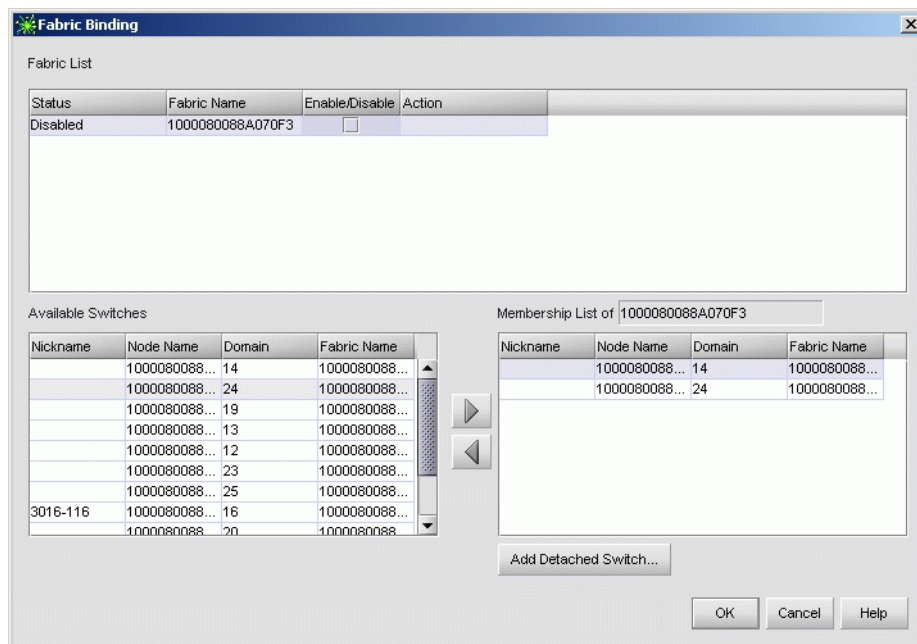


Figure 3-37 Fabric Binding Dialog Box

- b. At the *Fabric List* section, ensure the *Enable/Disable* checkbox is enabled (checked) for the fabric containing both switches.
- c. At the *Membership List of <Fabric Name>* section, update the membership list for both elements to ensure interswitch compatibility, then click *OK*. The fabric binding feature is consistently enabled for both switches.

Did updating the fabric membership lists solve the problem?

NO YES

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

31

A port connection is not allowed because of a switch binding mismatch. Switch membership lists must be compatible for both fabric elements.

- a. At the *Hardware View* ([Figure 3-10](#) on page 3-20) for each switch, click *Configure* and select *Switch Binding* and *Edit Membership List*. The *Switch Binding - Membership List* dialog box displays ([Figure 3-38](#)).

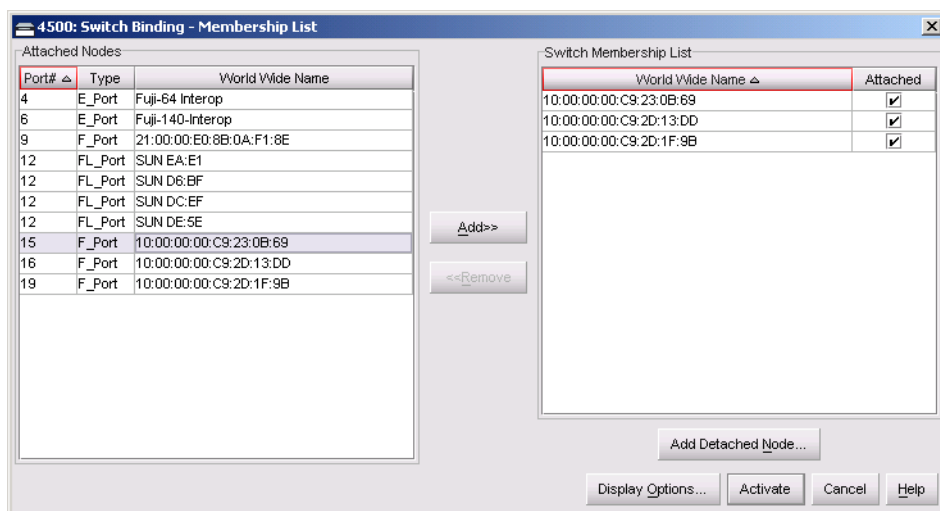


Figure 3-38 Switch Binding - Membership List Dialog Box

- b. At the *Switch Binding - Membership List* dialog box ensure the *Switch Membership List* is updated and correct for each switch, then click *Activate* for each switch. The switch binding feature is consistently enabled for both switches.

Did updating the switch membership lists solve the problem?

NO YES

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

32

A port connection is not allowed because of a Computer Network Technologies (CNT) wide area network (WAN) extension mode mismatch. Based on switch-to-switch differences between the ELP maximum frame sizes allowed, a connection was not allowed to a switch set to CNT WAN extension mode.

Contact McDATA support personnel to obtain software maintenance release 4.02.00. This release is required to correct the problem and allow McDATA switches to communicate with CNT UltraEdge WAN Gateways. **Exit MAP.**

33

The switch and attached device are performing a Fibre Channel link reset. This is a transient state. Wait approximately 30 seconds and inspect port state and LED behavior.

Did the link recover and resume operation?

NO YES

↓ The Fibre Channel link and switch appear operational.
Exit MAP.

Go to [step 1](#).

34

A link incident message appeared in the *Link Incident Log* or in the *Link Incident* field of the *Port Properties* dialog box; or an event code **581**, **582**, **583**, **584**, **585**, or **586** was observed at the console of an OSI server attached to the switch reporting the problem.

Clear the link incident for the port.

- a. At the *Hardware View* (Figure 3-10 on page 3-20), right-click the port. A pop-up menu appears.
- b. Select *Clear Link Incident Alert(s)*. The *Clear Link Incident Alert(s)* dialog box displays (Figure 3-39).

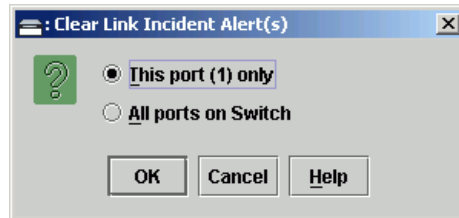


Figure 3-39 Clear Link Incident Alert(s) Dialog Box

- c. Select the *This port (n) only* radio button (where *n* is the port number) and click **OK**. The link incident clears.
- d. Monitor port operation for approximately five minutes.

Did the link incident recur?

YES NO

- ↓ The problem is transient and the Fibre Channel link and switch appear operational. **Exit MAP.**

35

Inspect the fiber-optic jumper cable attached to the port and ensure the cable is not bent and connectors are not damaged. If the cable is bent or connectors are damaged:

- a. Notify the customer the port will be blocked. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port and sets the attached device offline.
- b. Block the port. Refer to [Block or Unblock a Port](#) on page 4-51.
- c. Remove and replace the fiber-optic jumper cable.
- d. Unblock the port. Refer to [Block or Unblock a Port](#) on page 4-51.

Was a corrective action performed?

YES NO

- ↓ **Go to [step 37](#).**

36

Monitor port operation for approximately five minutes.

Did the link incident recur?

YES NO

↓ The Fibre Channel link and switch appear operational.
Exit MAP.

37

Clean fiber-optic connectors on the jumper cable.

- a. Notify the customer the port will be blocked. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port and sets the attached device offline.
- b. Block the port. Refer to [Block or Unblock a Port](#) on page 4-51.
- c. Disconnect both ends of the fiber-optic cable.
- d. Clean the fiber-optic connectors. Refer to [Clean Fiber-Optic Components](#) on page 4-54.
- e. Reconnect the fiber-optic cable.
- f. Unblock the port. Refer to [Block or Unblock a Port](#) on page 4-51.
- g. Monitor port operation for approximately five minutes.

Did the link incident recur?

YES NO

↓ The Fibre Channel link and switch appear operational.
Exit MAP.

38

Disconnect the fiber-optic jumper cable from the switch port and connect the cable to a spare port.

Is a link incident reported at the new port?

YES NO

↓ **Go to [step 40](#).**

39

The attached device is causing the recurrent link incident. Notify the customer of the problem and have the system administrator:

- a. Inspect and verify operation of the attached device.
- b. Repair the attached device if a failure is indicated.
- c. Monitor port operation for approximately five minutes.

Did the link incident recur?

YES NO

- ↓ The attached device, Fibre Channel link, and switch appear operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

40

The switch port reporting the problem is causing the recurrent link incident. The recurring link incident indicates port degradation and a possible pending failure. **Go to [step 6](#).**

MAP 0700: Fabric, ISL, and Segmented Port Problem Determination

This MAP describes isolation of fabric logout, interswitch link (ISL), and E_Port segmentation problems. Failure indicators include:

- An event code recorded at the SANpilot event log or Sphereon 4500 *Event Log* (management server).
- A segmentation reason associated with a Fibre Channel port at the SANpilot interface.
- A yellow triangle (attention indicator) appears adjacent to a port graphic at the alert panel of the *Hardware View*.
- A link incident message recorded in the *Link Incident Log* or *Port Properties* dialog box.

1

Was an event code **011, 021, 051, 052, 061, 062, 063, 070, 071, 072, 140, 142, or 150** observed at the SANpilot event log or at the Sphereon 4500 *Event Log* (management server)?

YES NO



Go to [step 3](#).

2

[Table 3-13](#) lists event codes, brief explanations of the codes, and associated steps that describe fault isolation procedures.

Table 3-13 MAP 700 Event Codes

Event Code	Explanation	Action
011	Login Server database invalid.	Go to step 9 .
021	Name Server database invalid.	Go to step 9 .
051	Management Server database invalid.	Go to step 10 .
052	Management Server internal error.	Go to step 10 .
061	Fabric Controller database invalid.	Go to step 11 .
062	Maximum interswitch hop count exceeded.	Go to step 12 .
063	Remote switch has too many ISLs.	Go to step 13 .
070	E_Port is segmented.	Go to step 14 .
071	Switch is isolated.	Go to step 14 .
072	E_Port connected to unsupported switch.	Go to step 22 .
140	Congestion detected on an ISL.	Go to step 23 .
142	Low BB_Credit detected on an ISL.	Go to step 24 .
150	Zone merge failure.	Go to step 25 .

3

Is fault isolation being performed through the SANpilot interface?

YES NO

↓ Fault isolation is being performed at the management server or customer-supplied server. **Go to step 6.**

4

Does the SANpilot interface appear operational?

YES NO

↓ Analysis for an Ethernet link, AC power distribution, or CTP failure is not described in this MAP. Go to [MAP 0000: Start MAP on page 3-6](#). If this is the second time at this step, contact the next level of support. **Exit MAP.**

5

Inspect the Fibre Channel port segmentation reason at the SANpilot interface.

- At the *View* panel, click the *Port Properties* tab. The *View* panel (*Port Properties* tab) displays.
- Click the port number (**0** through **23**) of the segmented port.
- Inspect the *Reason* field for the selected port.

Is the *Reason* field blank or does it display an **N/A** message?

NO YES

↓ The switch ISL appears operational. **Exit MAP.**

The *Reason* field displays a segmentation reason message. [Table 3-14](#) lists the reasons and associated steps that describe fault isolation procedures.

Table 3-14 Port Segmentation Reasons and Actions (SANpilot)

Segmentation Reason	Action
Incompatible operating parameters.	Go to step 15 .
Duplicate domain ID.	Go to step 16 .
Incompatible zoning configurations.	Go to step 17 .

Table 3-14 Port Segmentation Reasons and Actions (SANpilot)

Segmentation Reason	Action
Build fabric protocol error.	Go to step 18 .
No principal switch.	Go to step 20 .
No response from attached switch (hello timeout).	Go to step 21 .

6

At the management server, does a yellow triangle (attention indicator) appear adjacent to a Fibre Channel port graphic at the *Hardware View* ([Figure 3-10](#) on page 3-20)?

YES NO



The problem is transient and the switch-to-fabric element connection appears operational. **Exit MAP.**

7

Inspect the port state and LED status for all ports with an attention indicator.

- a. At the *Hardware View*, double-click the port graphic with the attention indicator. The *Port Properties* dialog box displays.
- b. Inspect the *Operational State* field at the *Port Properties* dialog box.

Does the *Operational State* field indicate **Segmented E_Port**?

YES NO



Analysis for other port or link incident problems is not described in this MAP. Go to [MAP 0600: Port Failure and Link Incident Analysis](#) on page 3-74. **Exit MAP.**

8

Inspect the *Reason* field at the *Port Properties* dialog box. [Table 3-15](#) lists port segmentation reasons and associated steps that describe fault isolation procedures.

Table 3-15 Port Segmentation Reasons and Actions (Management Server)

Segmentation Reason	Action
Incompatible operating parameters.	Go to step 15 .
Duplicate domain ID.	Go to step 16 .
Incompatible zoning configurations.	Go to step 17 .
Build fabric protocol error.	Go to step 18 .
No principal switch.	Go to step 20 .
No response from attached switch (hello timeout).	Go to step 21 .

9

A minor error occurred that caused the Fabric Services database to be re-initialized to an empty state. As a result, a disruptive fabric logout and login occurred for all attached devices. The following list explains the error:

- **Event code 011** - The Login Server database failed cyclic redundancy check (CRC) validation.
- **Event code 021** - The Name Server database failed CRC validation.

All attached devices resume operation after fabric login. Perform the data collection procedure and return the CD to McDATA for analysis.

Exit MAP.

10

A minor error occurred that caused the Management Server database to be re-initialized to an empty state. As a result, a disruptive server logout and login occurred for all attached devices. The following list explains the error:

- **Event code 051** - The Management Server database failed CRC validation.
- **Event code 052** - An internal operating error was detected by the Management Server subsystem.

All attached devices resume operation after Management Server login. Perform the data collection procedure and return the CD to McDATA for analysis. **Exit MAP.**

11

As indicated by an event code **061**, a minor error occurred that caused the Fabric Controller database to be re-initialized to an empty state and fail CRC validation. As a result, the switch briefly lost interswitch link capability.

All interswitch links resume operation after CTP reset. Perform the data collection procedure and return the CD to McDATA for analysis.

Exit MAP.

12

As indicated by an event code **062**, the Fabric Controller software detected a path to another fabric element (director or switch) in a multiswitch fabric that traverses more than three interswitch links (hops). Fibre Channel frames may persist in the fabric longer than timeout values allow.

Advise the customer of the problem and work with the system administrator to reconfigure the fabric so the path between any two fabric elements does not traverse more than three hops.

Did fabric reconfiguration solve the problem?

NO YES



The switch and multiswitch fabric appear operational.

Exit MAP.

Contact the next level of support. **Exit MAP.**

13

As indicated by an event code **063**, the Fabric Controller software detected an:

- Intrepid 6064 Director in a multiswitch fabric that has more than 48 ISLs attached.
- Other fabric element (other than an Intrepid 6140 Director) in a multiswitch fabric that has more than 32 ISLs attached.

Fibre Channel frames may be lost or routed in loops because of potential fabric routing problems. Advise the customer of the problem and work with the system administrator to reconfigure the fabric so that no director or switch elements have more than the proscribed number of ISLs.

Did fabric reconfiguration solve the problem?

NO **YES**

↓ The switch and multiswitch fabric appear operational.
Exit MAP.

Contact the next level of support. **Exit MAP.**

14

A **070** event code indicates an E_Port detected an incompatibility with an attached switch and prevented the switches from forming a multiswitch fabric. A segmented E_port cannot transmit Class 2 or Class 3 Fibre Channel traffic.

A **071** event code indicates the switch is isolated from all switches in a multiswitch fabric, and is accompanied by a **070** event code for each segmented E_Port. The **071** event code is resolved when all **070** events are corrected.

Obtain supplementary event data for each **070** event code.

- a. At the *Hardware View* ([Figure 3-10](#) on page 3-20), click *Logs* and select *Event Log*. The *Event Log* displays.
- b. Examine the first five bytes (**0** through **4**) of event data.
- c. Byte **0** specifies the switch port number (**00** through **23**) of the segmented E_port. Byte **4** specifies the segmentation reason as specified in [Table 3-16](#).

Table 3-16 Byte 4 Segmentation Reasons and Actions

Byte 4	Segmentation Reason	Action
01	Incompatible operating parameters.	Go to step 15 .
02	Duplicate domain ID.	Go to step 16 .
03	Incompatible zoning configurations.	Go to step 17 .
04	Build fabric protocol error.	Go to step 18 .
05	No principal switch.	Go to step 20 .
06	No response from attached switch (hello timeout).	Go to step 21 .

15

A switch E_Port segmented because the error detect time out value (E_D_TOV) or resource allocation time out value (R_A_TOV) is incompatible with the attached fabric element.

- a. Contact McDATA customer support or engineering personnel to determine the recommended E_D_TOV and R_A_TOV values for both switches.
- b. Notify the customer both switches will be set offline. Ensure the system administrator quiesces Fibre Channel frame traffic through the switches and sets attached devices offline.
- c. Set both switches offline. Refer to [Set the Switch Online or Offline](#) on page 4-48.
- d. At the *Hardware View* ([Figure 3-10](#) on page 3-20) for the first switch reporting the problem, click *Configure* and select *Operating Parameters* and *Fabric Parameters*. The *Configure Fabric Parameters* dialog box displays ([Figure 3-40](#) on page 3-100).

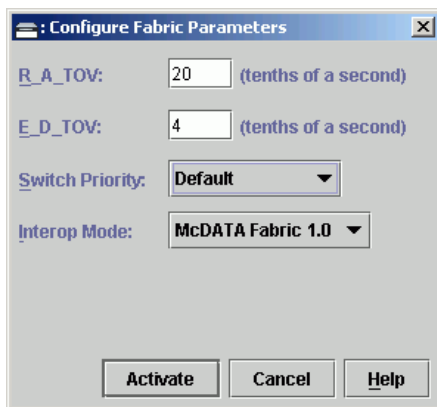


Figure 3-40 Configure Fabric Parameters Dialog Box

- e. Type the recommended E_D_TOV and R_A_TOV values, then click *Activate*.
- f. Repeat steps d and e at the *Hardware View* for the switch attached to the segmented E_Port (second switch). Use the same E_D_TOV and R_A_TOV values.

- g. Set both switches online. Refer to [Set the Switch Online or Offline](#) on page 4-48.

Did the operating parameter change solve the problem and did both switches join through the ISL to form a fabric?

NO YES

- ↓ The switch, associated ISL, and multiswitch fabric appear operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

16

A switch E_Port segmented because two fabric elements had duplicate domain IDs.

- Work with the system administrator to determine the desired domain ID (**1** through **31** inclusive) for each switch.
- Notify the customer both switches will be set offline. Ensure the system administrator quiesces Fibre Channel frame traffic through the switches and sets attached devices offline.
- Set both switches offline. Refer to [Set the Switch Online or Offline](#) on page 4-48.
- At the *Hardware View* ([Figure 3-10](#) on page 3-20) for the first switch reporting the problem, click *Configure* and select *Operating Parameters* and *Switch Parameters*. The *Configure Switch Parameters* dialog box displays ([Figure 3-41](#)).

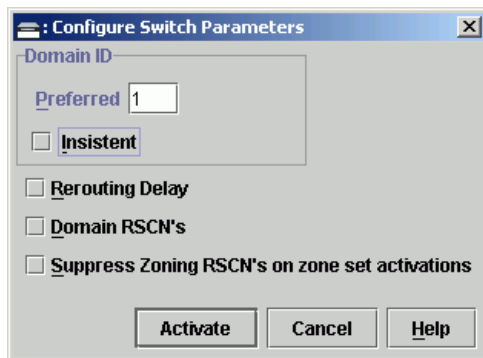


Figure 3-41 Configure Switch Parameters Dialog Box

- e. Type the customer-determined preferred domain ID value, then click *Activate*.
- f. Repeat steps d and e at the *Hardware View* for the switch attached to the segmented E_Port (second switch). Use a different preferred domain ID value.
- g. Set both switches online. Refer to [Set the Switch Online or Offline](#) on page 4-48.

Did the domain ID change solve the problem and did both switches join through the ISL to form a fabric?

NO YES

- ↓ The switch, associated ISL, and multiswitch fabric appear operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

17

A switch E_Port segmented because two switches had incompatible zoning configurations. An identical zone name is recognized in the active zone set for both switches, but the zones contain different members.

- a. Work with the system administrator to determine the desired zone name change for one of the affected switches. Zone names must conform to the following rules:
 - The name must be 64 characters or fewer in length.
 - The first character must be a letter (**a** through **z**), upper or lower case.
 - Other characters must be alphanumeric (**a** through **z** or **0** through **9**), dollar sign (**\$**), hyphen (**-**), caret (**^**), or underscore (**_**).
- b. Close the Element Manager application (*Hardware View*). The SANavigator or EFCM main window (still active) displays.
- c. At the SANavigator or EFCM main window physical map, right-click the blue background representing the fabric containing the switch reporting the problem. A pop-up menu appears.
- d. Select the *Zoning* option from the menu. The *Zoning* dialog box displays with the *Zone Library* page open ([Figure 3-42](#)).

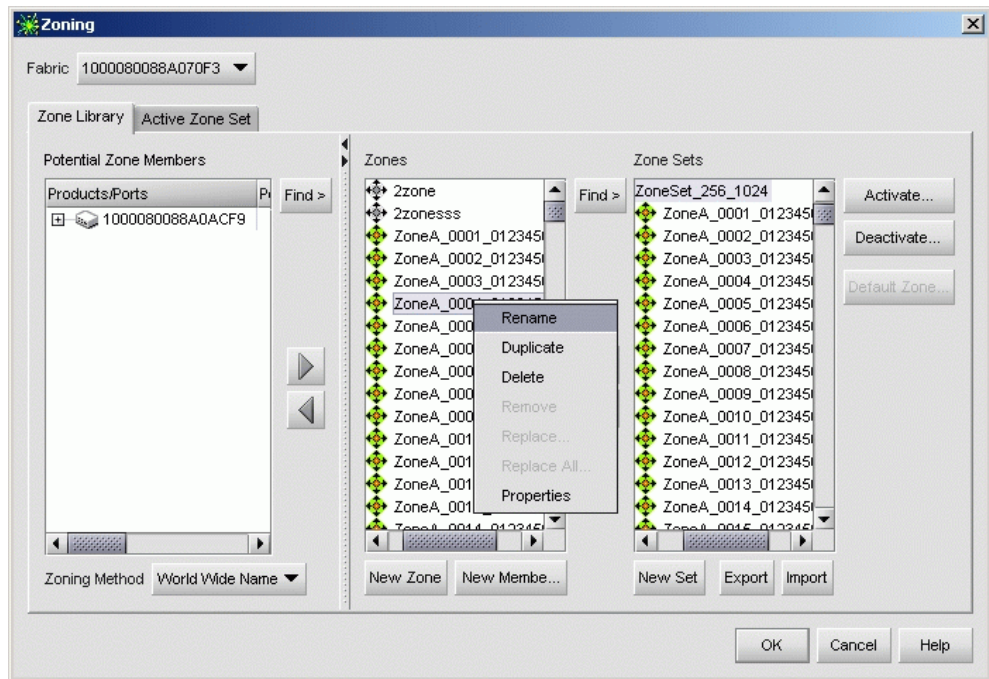


Figure 3-42 Zoning Dialog Box (Zone Library Tab)

- e. Click the *Active Zone Set* tab. The *Zoning* dialog box displays with the *Active Zone Set* page open (Figure 3-43).

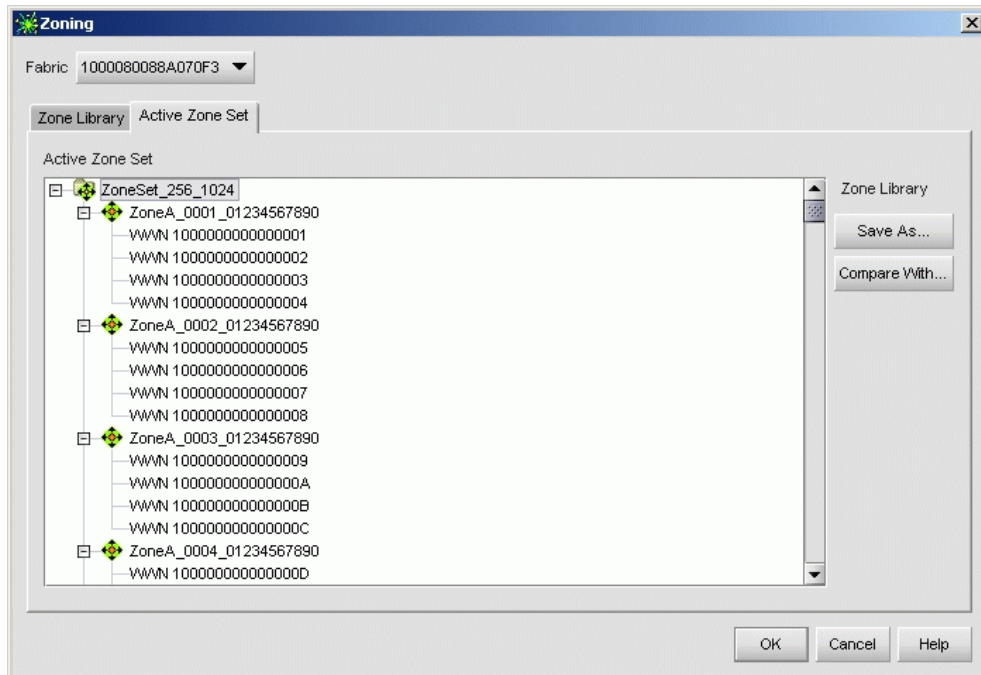


Figure 3-43 Zoning Dialog Box (Active Zone Set Tab)

- f. Inspect zone names in the active zone set to determine the incompatible name.
- g. Modify the incompatible zone name as directed by the customer:
 1. At the *Zoning* dialog box, click the *Zone Library* tab. The dialog box returns to the *Zone Library* page (Figure 3-42 on page 3-103).
 2. At the *Zones* field, right-click the zone name to be changed. A pop-up menu appears.
 3. Select the *Rename* option from the menu. The selected zone name remains highlighted in blue. Type the new zone name (specified by the customer), then click *OK* to activate the change and close the *Zoning* dialog box.

Did the zone name change solve the problem and did both switches join through the ISL to form a fabric?

NO YES

↓ The switch, associated ISL, and multiswitch fabric appear operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

18

A switch E_Port segmented because a build fabric protocol error was detected.

- a. Disconnect the fiber-optic jumper cable from the segmented E_Port.
- b. Reconnect the cable to the same port.

Did disconnecting and reconnecting the cable solve the problem and did both switches join through the ISL to form a fabric?

NO YES

↓ The switch, associated ISL, and multiswitch fabric appear operational. **Exit MAP.**

19

Initial program load (IPL) the switch. Refer to [IML, IPL, or Reset the Switch](#) on page 4-56.

Did the IPL solve the problem and did both switches join through the ISL to form a fabric?

NO YES

↓ The switch, associated ISL, and multiswitch fabric appear operational. **Exit MAP.**

Perform the data collection procedure and contact the next level of support. **Exit MAP.**

20

A switch E_Port segmented because no switch in the fabric is capable of becoming the principal switch.

- a. Notify the customer the switch will be set offline. Ensure the system administrator quiesces Fibre Channel frame traffic through the switch and sets attached devices offline.

- b. Set the switch offline. Refer to [Set the Switch Online or Offline](#) on page 4-48.
- c. At the *Hardware View* ([Figure 3-10](#) on page 3-20) for the switch reporting the problem, click *Configure* and select *Operating Parameters* and *Fabric Parameters*. The *Configure Fabric Parameters* dialog box displays ([Figure 3-40](#) on page 3-100).
- d. At the *Switch Priority* field, select *Principal*, *Never Principal*, or *Default* (the default setting is *Default*). The switch priority value designates the fabric's principal switch. The principal switch is assigned a priority of 1 and controls the allocation and distribution of domain IDs for all fabric switches (including itself).

Principal is the highest priority setting, *Default* is the next highest, and *Never Principal* is the lowest priority setting. The setting *Never Principal* means that the switch is incapable of becoming a principal switch. If all switches are set to *Principal* or *Default*, the switch with the highest priority and the lowest WWN becomes the principal switch.

At least one switch in a multiswitch fabric must be set as *Principal* or *Default*. If all switches are set to *Never Principal*, all ISLs segment and the message *No Principal Switch* appears in the *Reason* field of the *Port Properties* dialog box.

- e. Set the switch online. Refer to [Set the Switch Online or Offline](#) on page 4-48.

Did the switch priority change solve the problem and did both switches join through the ISL to form a fabric?

NO YES

↓ The switch, associated ISL, and multiswitch fabric appear operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

21

A switch *E_Port* segmented (at an operational switch) because a response (hello timeout) to a verification check indicates an attached switch is not operational.

- a. Perform the data collection procedure at the operational switch and return the CD to McDATA for analysis. This information may assist in fault isolating the failed switch.
- b. Go to [MAP 0000: Start MAP](#) on page 3-6 and perform fault isolation for the failed switch.

Exit MAP.

22

As indicated by an event code **072**, a switch E_Port is connected to an unsupported switch or fabric element.

Advise the customer of the problem and disconnect the interswitch link to the unsupported switch. **Exit MAP.**

23

A **140** event code occurs only if the optional OpenTrunking feature is enabled. The event code indicates OpenTrunking firmware detected an ISL with Fibre Channel traffic that exceeds the configured congestion threshold.

No action is required for an isolated event. However, if this event persists, perform one of the following:

- Relieve the congestion by adding parallel ISLs between the switches reporting the problem.
- Increase the ISL link speed between the switches reporting the problem (from 1 Gbps to 2 Gbps).
- Reroute Fibre Channel traffic by moving device connections to a less-congested region of the fabric.

Did the corrective action solve the problem and relieve the reported ISL congestion?

NO YES

↓ The ISL appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

24

A **142** event code occurs only if the optional OpenTrunking feature is enabled. The event code indicates OpenTrunking firmware detected an ISL with no transmission BB_Credit for a period of time that exceeded the configured low BB_Credit threshold. This results in downstream fabric congestion.

No action is required for an isolated event or if the reporting ISL approaches 100% throughput. However, if this event persists, perform one of the following:

- Relieve the congestion by adding parallel ISLs between the switches reporting the problem.

- Increase the ISL link speed between the switches reporting the problem (from 1 Gbps to 2 Gbps).
- Reroute Fibre Channel traffic by moving device connections to a less-congested region of the fabric.

Did the corrective action solve the problem and relieve the reported low BB_Credit condition?

NO YES

↓ The ISL appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

25

A **150** event code indicates a zone merge process failed during ISL initialization. Either an incompatible zone set was detected or a problem occurred during delivery of a zone merge frame. This event code always precedes a **070** event code, and represents the reply of an adjacent fabric element in response to a zone merge frame.

Obtain supplementary event data for each **150** event code.

- At the *Hardware View* ([Figure 3-10](#) on page 3-20), click *Logs* and select *Event Log*. The *Event Log* displays.
- Examine the first 12 bytes (**0** through **11**) of event data.
- Bytes **0** through **3** specify the E_Port number (**00** through **23**) reporting the problem. Bytes **8** through **11** specify the failure reason as specified in [Table 3-17](#) on page 3-108.

Table 3-17 Bytes 8 through 11 Failure Reasons and Actions

Bytes 8 - 11	Failure Reason	Action
01	Invalid data length.	Go to step 26 .
08	Invalid zone set format.	Go to step 26 .
09	Invalid data.	Go to step 27 .
0A	Cannot merge.	Go to step 27 .
F0	Retry limit reached.	Go to step 26 .
F1	Invalid response length.	Go to step 26 .
F2	Invalid response code.	Go to step 26 .

26

A zone merge process failed during ISL initialization. The following list explains the reason:

- **Failure reason 01** - An invalid data length condition caused an error in a zone merge frame.
- **Failure reason 08** - An invalid zone set format caused an error in a zone merge frame.
- **Failure reason F0** - A retry limit reached condition caused an error in a zone merge frame.
- **Failure reason F1** - An invalid response length condition caused an error in a zone merge frame.
- **Failure reason F2** - An invalid response code caused an error in a zone merge frame.

Disconnect the fiber-optic jumper cable from the E_Port reporting the problem, then reconnect the cable to the same port.

Did disconnecting and reconnecting the cable solve the problem and was the resulting zone merge process successful?

NO YES

↓ The merged zone appears operational. **Exit MAP.**

Perform the data collection procedure and return the CD to McDATA for analysis. Contact the next level of support. **Exit MAP.**

27

A zone merge process failed during ISL initialization. The following list explains the reason:

- **Failure reason 09** - Invalid data caused a zone merge failure.
- **Failure reason 0A** - A *Cannot Merge* condition caused a zone merge failure.

Obtain supplementary error code data for the **150** event code.

- a. At the *Hardware View* ([Figure 3-10](#) on page 3-20), click *Logs* and select *Event Log*. The *Event Log* displays.
- b. Examine bytes **12** through **15** of event data that specify the error code. Record the error code.

Perform the data collection procedure and return the CD to McDATA for analysis. Contact the next level of support, and report the **150** event code, the associated failure reason, and the associated error code. **Exit MAP.**

MAP 0800: Server Hardware Problem Determination

This MAP describes isolation of hardware-related problems with the customer-supplied server communicating with the switch through the SANpilot interface, management server, or customer-supplied server running the SAN management application.

The MAP provides high-level fault isolation instructions only. Refer to the documentation provided with the server for detailed problem determination and resolution.

To fault isolate software-related problems with the server, go to [MAP 0300: Server Application Problem Determination](#) on page 3-41.

To fault isolate switch-to-server communication problems, go to [MAP 0400: Loss of Server Communication](#) on page 3-51.

1

Are you performing fault isolation at a customer-supplied server communicating with the switch through the SANpilot interface?

NO YES



The server and Internet browser application are not McDATA-supported and analysis for the failure is not described in this MAP. Refer to the supporting documentation shipped with the server for instructions on resolving the problem. **Exit MAP.**

2

Are you performing fault isolation at a customer-supplied, Unix-based server running the client SAN management application?

NO YES



Unix-based servers are not McDATA-supported and analysis for the failure is not described in this MAP. Refer to the supporting documentation shipped with the server for instructions on resolving the problem. **Exit MAP.**

3

Are you performing fault isolation at one of the following servers?

- The rack-mount management server running the Windows 2000 Professional operating system.
- A customer-supplied server running the client SAN management application and a Windows-based operating system (Windows 95, Windows 98, Windows 2000, Windows XP, or Windows NT 4.0).
- A customer-supplied server running the EFCM Lite application and a Windows-based operating system.

YES NO

↓ Analysis for the server failure is not described in this MAP.
Contact the next level of support. **Exit MAP.**

4

At the server, close the SAN management or EFCM Lite application.

- a. Select *Shutdown* from the *SAN* menu. A *SANavigator* or *EFCM Message* dialog box displays (Figure 3-44).

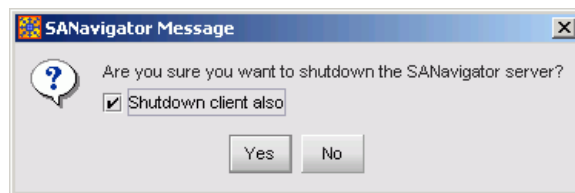


Figure 3-44 SANavigator or EFCM Message Dialog Box

- b. Click *Yes* to close the SAN management application.
- c. Close any other applications.

Continue to the next step.

5

Inspect the available random access memory (RAM). The server must have a minimum of 128 megabytes (MB) of memory to run the Windows-based operating system and SAN management application.

- a. Right-click anywhere on the Windows task bar at the bottom of the desktop. A pop-up menu appears.
- b. Select *Task Manager*. The *Windows Task Manager* dialog box displays with the *Applications* page open by default. Click the *Performance* tab to open the *Performance* page (Figure 3-45).

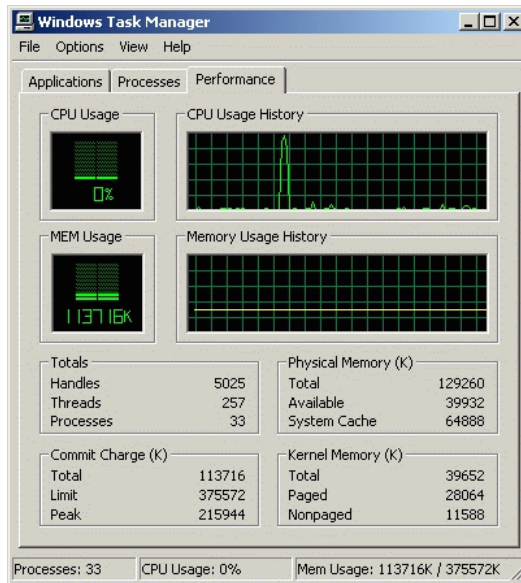


Figure 3-45 Windows Task Manager Dialog Box (Performance Page)

- c. At the *Physical Memory (K)* portion of the dialog box, inspect the total amount of physical memory.
- d. Close the dialog box by clicking *Close (X)* at the upper right corner of the window.

Does the computer have sufficient memory?

YES NO



A memory upgrade is required. Inform the customer of the problem and contact the next level of support. **Exit MAP.**


6

Reboot the server and perform system diagnostics.

- a. At the Windows 2000 desktop, click *Start* at the left side of the task bar (bottom of the desktop), then select *Shut Down*. The *Shut Down Windows* dialog box displays (Figure 3-46).



Figure 3-46 Shut Down Windows Dialog Box

- b. Select the *Shut Down* option from the list box and click *OK*. The management server powers down.
- c. Wait approximately 30 seconds and press the power () button on the LCD panel to power on the server and perform POSTs. During POSTs:
 1. The green LCD panel illuminates.
 2. The green **HDD** LED blinks momentarily, and processor speed and random-access memory information display momentarily at the LCD panel.
 3. After a few seconds, the LCD panel displays the following message pertaining to boot sequence selection (Figure 3-47):

Boot from LAN?
Press <Enter>

Figure 3-47 LCD Panel During Boot Sequence

4. Ignore the message. After ten seconds, the server performs the boot sequence from BIOS. During the boot sequence, the server performs additional POSTs and displays the following operational information at the LCD panel:

- Host name.
- System date and time.
- LAN 1 and LAN 2 IP addresses.
- Fan 1, fan 2, fan 3, and fan 4 rotational speed.
- CPU temperature.
- Hard disk capacity.
- Virtual and physical memory capacity.

d. After successful POST completion, the LCD panel displays a **Welcome!!** message, then continuously cycles through and displays server operational information.

Did POSTs detect a problem?

NO YES

↓

A computer hardware problem exists. Refer to the supporting documentation shipped with the server for instructions on resolving the problem. **Exit MAP.**

7

After rebooting the server at the LCD panel, log on to the management server's Windows 2000 desktop through a LAN connection to a browser-capable PC. Refer to [Access the Management Server Desktop](#) on page 2-55 for instructions. The SAN management application starts and the *SANavigator Log In* or *EFCM Log In* dialog box displays ([Figure 3-48](#) on page 3-115).

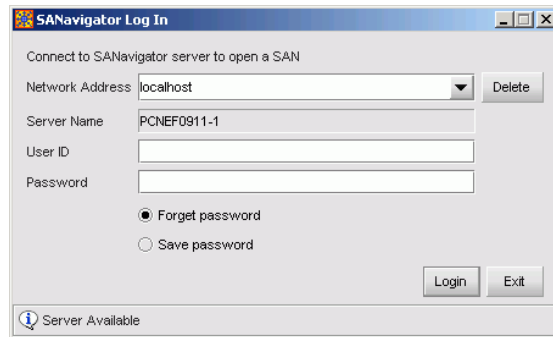


Figure 3-48 SANavigator Login or EFCM Login Dialog Box

Did the *SANavigator Log In* or *EFCM Log In* dialog box display?

YES NO



Go to [step 9](#).

8

At the *SANavigator Log In* or *EFCM Log In* dialog box, type a user ID and password (obtained in [MAP 0000: Start MAP](#), and both are case sensitive), and click *Login*. The SAN management application opens and the SANavigator or EFCM main window displays ([Figure 3-9](#) on page 3-17).

Did the main window display and does the SAN management application appear operational?

NO YES



The server appears operational. **Exit MAP.**

9

Perform one of the following:

- If the server has standalone diagnostic test programs resident on the hard drive, perform the diagnostics. Refer to supporting documentation shipped with the server for instructions.
- If the server does not have standalone diagnostic test programs resident on hard drive, **go to [step 10](#)**.


Did diagnostic test programs detect a problem?

NO YES

↓ Refer to the supporting documentation shipped with the server for instructions to resolve the problem. **Exit MAP.**

10

Reboot the server.

- a. At the Windows 2000 desktop, click *Start* at the left side of the task bar (bottom of the desktop), then select *Shut Down*. The *Shut Down Windows* dialog box displays (Figure 3-46 on page 3-113).
- b. Select the *Shut Down* option from the list box and click *OK*. The management server powers down.
- c. Wait approximately 30 seconds and press the power () button on the LCD panel to power on the server and perform POSTs. During POSTs:
 1. The green LCD panel illuminates.
 2. The green **HDD** LED blinks momentarily, and processor speed and random-access memory information display momentarily at the LCD panel.
 3. After a few seconds, the LCD panel displays the following message pertaining to boot sequence selection (Figure 3-49):



Boot from LAN?
Press <Enter>

Figure 3-49 LCD Panel During Boot Sequence

4. Ignore the message. After ten seconds, the server performs the boot sequence from BIOS. During the boot sequence, the server performs additional POSTs and displays the following operational information at the LCD panel:
 - Host name.
 - System date and time.
 - LAN 1 and LAN 2 IP addresses.
 - Fan 1, fan 2, fan 3, and fan 4 rotational speed.

- CPU temperature.
 - Hard disk capacity.
 - Virtual and physical memory capacity.
- d. After successful POST completion, the LCD panel displays a **Welcome!!** message, then continuously cycles through and displays server operational information.
- e. After rebooting the server at the LCD panel, log on to the management server's Windows 2000 desktop through a LAN connection to a browser-capable PC. Refer to [Access the Management Server Desktop](#) on page 2-55 for instructions. The SAN management application starts and the *SANavigator Log In* or *EFCM Log In* dialog box displays ([Figure 3-48](#) on page 3-115).
- f. At the *SANavigator Log In* or *EFCM Log In* dialog box, type a user ID and password (obtained in [MAP 0000: Start MAP](#), and both are case sensitive), and click *Login*. The SAN management application opens and the SANavigator or EFCM main window displays ([Figure 3-9](#) on page 3-17).

Did the main window display and does the SAN management application appear operational?

NO YES



The server appears operational. **Exit MAP.**

11

Re-install the SAN management application. Refer to [Install or Upgrade Software](#) on page 4-87 for instructions.

Did the SAN management application install and open successfully?

NO YES



The server appears operational. **Exit MAP.**

12

Advise the customer and next level of support that the server hard drive should be restored to its original factory configuration. If the customer and support personnel do not concur, **go to step 13**.

- a. Format the server hard drive. Refer to supporting documentation shipped with the server for instructions.
- b. Install the Windows 2000 operating system and SAN management application. Refer to [Appendix C, Restore Management Server](#) for instructions.

Did the server hard drive format, and did the operating system and SAN management application install and open successfully?

NO YES



The server appears operational. **Exit MAP.**

13

Additional analysis for the failure is not described in this MAP. Contact the next level of support. **Exit MAP.**

This chapter describes repair-related procedures for the Sphereon 4500 Fabric Switch and associated field-replaceable units (FRUs). The procedures are performed through the SANpilot interface, storage area network (SAN) management application (SANavigator 4.0 or EFCM 8.0), or Sphereon 4500 Element Manager application. The following procedures are described:

- Obtain log information.
- Obtain port diagnostic information.
- Perform port diagnostic loopback tests.
- Collect maintenance data.
- Set the switch online or offline.
- Block or unblock Fibre Channel ports.
- Clean fiber-optic components.
- Power the switch on and off.
- Perform a switch reset, initial machine load (IML), or initial program load (IPL).
- Manage firmware versions.
- Manage configuration data.
- Install or upgrade software.

Do not perform repairs until a failure is isolated to a FRU. If fault isolation was not performed, refer to [MAP 0000: Start MAP](#) on page 3-6.

Procedural Notes

The following procedural notes are referenced in applicable repair procedures. The notes do not necessarily apply to all procedures in the chapter.

1. Before performing a procedure, read the procedure carefully and thoroughly to familiarize yourself with the information and reduce the possibility of problems or customer down time.
2. When performing procedures described in this chapter, follow all **WARNING** statements, and statements listed in the preface of this manual.
3. After completing steps of a detailed procedure that is referenced from another procedure, return to the initial (referencing) procedure and continue to the next step of that procedure.

Repair Procedures

Use the following repair-related procedures when using either the SANpilot interface or the 1U, rack-mount management server (running SAN management and Element Manager applications) to manage your Sphereon 4500 Fabric Switch. Procedures for the SANpilot interface are presented first, followed by the management server procedure for the same task. Some tasks not supported by the SANpilot interface are represented only by management server procedures.

Obtain Log Information

The SANpilot interface, SAN management application, and Sphereon 4500 Element Manager application provide access to logs that contain information for maintenance personnel. Logs are available as follows:

- The SANpilot interface provides access to the following:
 - Event Log.
 - Open Trunking Re-Route Log.
 - Link Incident Log.
 - Security Log

- Audit Log
- Fabric Log
- Embedded Port Frame Log
- The SAN management application (SANavigator 4.0 or EFCM 8.0) provides access to the following:
 - Audit Log.
 - Event Log.
 - Session Log.
 - Product Status Log.
 - Fabric Log.
- The Element Manager application provides access to the following:
 - Sphereon 4500 Audit Log.
 - Sphereon 4500 Event Log.
 - Hardware Log.
 - Link Incident Log.
 - Threshold Alert Log.
 - Open Trunking Log.

SANpilot Logs

To open a SANpilot log, click the *Logs* tab at the *Monitor* panel. The *Monitor* panel opens with the *Logs* page displayed ([Figure 4-1](#)).

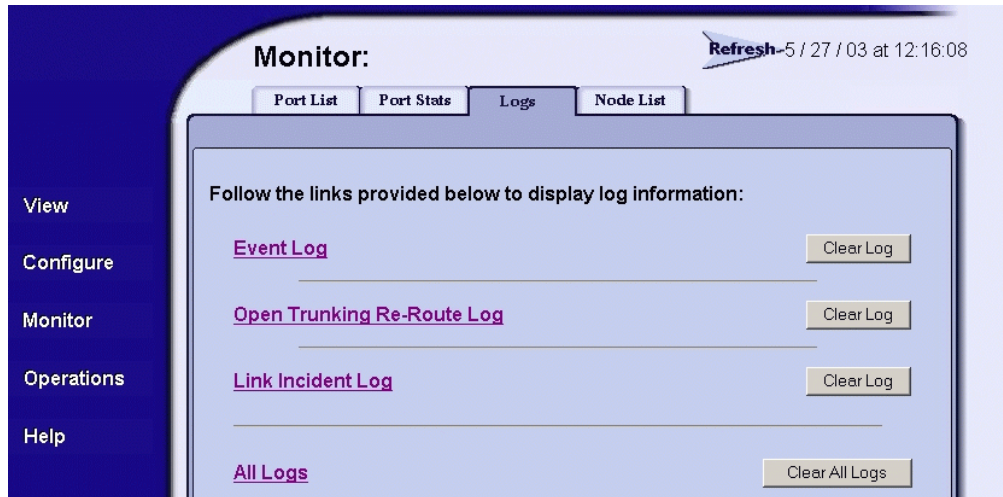


Figure 4-1 Monitor Panel (Logs Page)

At the *Logs* page:

- Select (double-click) a log title to open and view the contents of the associated log, or
- Select (double-click) the *All Logs* title to open and simultaneously view the contents of all logs.

The *Logs* page provides a *Clear Log* button for each log. Click the button to delete all entries for the associated log. The *Logs* page also provides a *Clear All Logs* button. Click the button to delete all entries in all logs.

Event Log

The *Event Log* (Figure 4-2) displays events or errors recorded at the SANpilot interface. Entries reflect the status of the interface and managed switch. The log stores up to 200 entries, and the most recent entry appears at the top of the log.

Date/Time	Error Code	Severity	Event Data
5/28/03 2:46 pm	410	Informational	44
5/28/03 2:46 pm	453	Informational	0480 0000 0000 0000 0000 0000 0000 0000
5/28/03 2:46 pm	421	Informational	3036 2E30 302E 3030 2031 3900 0000 0000
5/28/03 2:44 pm	423	Informational	
5/28/03 2:43 pm	410	Informational	44
5/28/03 2:43 pm	453	Informational	0480 0000 0000 0000 0000 0000 0000 0000
5/28/03 2:43 pm	421	Informational	3036 2E30 302E 3030 2031 3900 0000 0000
5/28/03 2:40 pm	423	Informational	

Figure 4-2 Event Log

The log consists of the following columns:

- **Date/Time** - Date and time the event occurred.
- **Error Code** - Three-digit code that describes the event. Event codes are listed and described in [Appendix B, Event Code Tables](#).
- **Severity** - Severity of the event (*Informational, Minor, Major, or Severe*).
- **Event Data** - Up to 32 bytes of supplementary information (if available) in hexadecimal format. Event data is described in [Appendix B, Event Code Tables](#).

Open Trunking Re-Route Log

The *Open Trunking Re-Route Log* ([Figure 4-3](#)) displays interswitch link (ISL) congestion events that cause Fibre Channel traffic to be routed through an alternate ISL. Entries reflect the traffic re-route status at the managed switch. The log stores up to 200 entries, and the most recent entry appears at the top of the log.

Date/Time	Receive Port	Target Domain	Old Exit Port	New Exit Port
5/27/03 12:18 pm	16	5	3	6
5/27/03 12:18 pm	15	4	2	5
5/27/03 11:32 am	16	5	3	6
5/27/03 11:32 am	15	4	2	5
5/27/03 11:31 am	16	5	3	6
5/27/03 11:31 am	15	4	2	5

Figure 4-3 Open Trunking Re-Route Log

The log consists of the following columns:

- **Date/Time** - Date and time the re-route action occurred.
- **Receive Port** - The switch port number (decimal) used for receiving Fibre Channel traffic after the re-route action.
- **Target Domain** - The domain ID (decimal) of the target device to which Fibre Channel traffic from the switch was rerouted.
- **Old Exit Port** - The switch port number (decimal) used for transmitting Fibre Channel traffic before the re-route action.
- **New Exit Port** - The switch port number (decimal) used for transmitting Fibre Channel traffic after the re-route action.

Link Incident Log

The *Link Incident Log* (Figure 4-4 on page 4-7) displays Fibre Channel link incident events recorded at the SANpilot interface. Entries reflect the cause of the link incident. The log stores up to 200 entries, and the most recent entry appears at the top of the log.

Link Incident Log		
Date/Time	Port	Event
5/28/03 3:27 pm	5	Loss-of-Signal or Loss-of-Synchronization.
5/28/03 3:27 pm	13	Loss-of-Signal or Loss-of-Synchronization.
5/28/03 3:27 pm	15	Loss-of-Signal or Loss-of-Synchronization.

Figure 4-4 Link Incident Log

The log consists of the following columns:

- **Date/Time** - Date and time the link incident occurred.
- **Port** - Port number (0 through 23) that reported the link incident.
- **Event** - Brief description of the link incident. Problem descriptions include:
 - Implicit incident.
 - Bit-error threshold exceeded.
 - Loss of signal or loss of synchronization.
 - Not-operational primitive sequence received.
 - Primitive sequence timeout.
 - Invalid primitive sequence received for current link state.

Refer to [MAP 0600: Port Failure and Link Incident Analysis](#) on page 3-74 for corrective actions in response to these link incident messages.

Viewing the Security Log

Select *Monitor* on the navigation panel. Select the *Logs* tab; the *Logs* tab view displays. Select the *Security Log* link. The Security Log displays in text format, as shown in [Figure 4-5](#). The log displays in a separate browser window. Close the browser window to close the log.

The security log provides:

- **Reason:** The reason code for the security Event

- **Date/Time:** The date/time when the event occurred.
- **Trigger Level:** The trigger level of the event. Possible values include: Informational, Security Change, or Error
- **Count:** A cumulative count of events within a known period.
- **Category:** The event category message with possible values may be: Successful Connection, Disconnection, Configuration Change, Authorization Failure, Authentication Failure, or Reserved
- **Description:** Description of the event.
- **Data:** Any extra or event specific data.

Security Log			
Reason	Date/Time	Trigger Level	Count
10000	09/30/2004 11:47:12	Informational	1
Category: Successful Connection			
Description: EWS User Connected			
Data: User name = 'Administrator' IP address = 127.000.000.001 Role = administrator Protocol = http			
10400	09/30/2004 11:47:05	Error	1
Category: Authentication Failure			
Description: EWS Wrong User Name - Password Combination			
Data: User name = 'Administrator' IP address = 127.000.000.001			
10000	09/30/2004 11:46:59	Informational	1
Category: Successful Connection			
Description: EWS User Connected			
Data: User name = 'Administrator' IP address = 127.000.000.001 Role = administrator Protocol = http			

Figure 4-5 Security Log

Clearing the Security Log

ATTENTION! Before clearing logs, make sure the logs are not needed for troubleshooting. Once a log is cleared, the data cannot be retrieved.

To clear the Security Log, select *Monitor* and select the *Logs* tab. Select the *Clear Log* button, next to the Security Log link. A message displays stating that the operation has been performed successfully.

Viewing the Audit Log

Select *Monitor* on the navigation panel. Select the *Logs* tab; the *Logs* tab view displays. Select the *Audit Log* link. The Audit Log displays in text format, as shown in [Figure 4-6](#). The log displays in a separate browser window. Close the browser window to close the log.

The audit lot provides:

- Date/Time: The date and time of the log entry.
- Source: The source of Audit Log event.
- User ID: Identifier of the user that issued the command. The identifier is usually an IP Address.
- Action: The type of Audit Log event.

Audit Log Date/Time	Source	User Id
09/30/2004 11:47:05:00	HTTP	127.0.0.1
Action: Authentication user modified		
09/30/2004 11:45:49:00	Internal	
Action: Port BB credit has changed		
09/30/2004 11:45:49:00	Internal	
Action: Port 60: Speed set to 10 Gb/sec		
09/30/2004 11:45:49:00	Internal	
Action: Port BB credit has changed		
09/30/2004 11:45:49:00	Internal	
Action: Port 44: Speed set to 10 Gb/sec		
09/30/2004 11:45:49:00	Internal	
Action: Port BB credit has changed		
09/30/2004 11:45:49:00	Internal	
Action: Port 28: Speed set to 10 Gb/sec		
09/30/2004 11:45:49:00	Internal	
Action: Active Address Configuration modified		
09/30/2004 11:45:49:00	Internal	
Action: Active Address Configuration modified		
09/30/2004 11:45:49:00	Internal	
Action: Active Address Configuration modified		
09/30/2004 11:45:49:00	Internal	
Action: Active Address Configuration modified		
09/30/2004 11:45:49:00	Internal	

Figure 4-6 Viewing the Audit Log

Clearing the Audit Log

ATTENTION! Before clearing logs, make sure the logs are not needed for troubleshooting. Once a log is cleared, the data cannot be retrieved.

To clear the Audit Log, select *Monitor* and select the *Logs* tab. Select the *Clear Log* button, next to the Audit Log link. A message displays stating that the operation has been performed successfully.

Viewing the Fabric Log

Select *Monitor* on the navigation panel. Select the *Logs* tab; the *Logs* tab view displays. Select the *Fabric Log*, either a wrapped or non-wrapped view. TheFabric Log displays in text format, as shown in Figure 4-7. The log displays in a separate browser window. Close the browser window to close the log.

TIP: The same entries will go into both logs until the non-wrap log gets full. Once the non-wrap log gets full, the entries go into the wrap log. Once the wrap log is full, it will start to overwrite entries. If you need to look at a history of log entries, you should review both logs.

The Fabric Log provides:

- Count: A cumulative count of entries within a known period.
- Date/Time: The date and time of the log entry.
- Description: A description of the log entry.
- Data: Extended data that is associated with the log entry.

```
Non-Wrapping Fabric Log
Count      Date/Time
-----
10         09/30/2004 11:46:03
  Description: Fabric Operational
  Data:
9          09/30/2004 11:46:03
  Description: Paths Operational
  Data:
8          09/30/2004 11:46:03
  Description: Zone Merge Completed
  Data:
7          09/30/2004 11:46:03
  Description: Notified by Fabric controller and discover new or changed E_Port
              to start zone merge
  Data:
6          09/30/2004 11:46:03
  Description: Path Selection Completed
  Data:
5          09/30/2004 11:46:03
  Description: Domain ID Change
  Data:      New Domain ID=0001, Preferred Domain ID=0001
```

Figure 4-7 Viewing the Fabric Log

Clearing the Fabric Log

ATTENTION! Before clearing logs, make sure the logs are not needed for troubleshooting. Once a log is cleared, the data cannot be retrieved.

To clear the Fabric Log, select *Monitor* and select the *Logs* tab. Select the *Clear Log* button, next to the Fabric Log link. A message displays stating that the operation has been performed successfully.

Viewing the Embedded Port Frame Log

Select *Monitor* on the navigation panel. Select the *Logs* tab; the *Logs* tab view displays. Select the *Embedded Port Frame Log* link either a wrapped or non-wrapped view. The Frame Logs listing displays in text format, as shown in [Figure 4-10](#). The log displays in a separate browser window. Close the browser window to close the log.

TIP: The same entries will go into both logs until the non-wrap log gets full. Once the non-wrap log gets full, the entries go into the wrap log. Once the wrap log is full, it will start to overwrite entries. If you need to look at a history of log entries, you should review both logs.

The Embedded Port Frame Log provides:

- Count: A cumulative count of entries within a known period.
- Date/- Time: Time of the frame.
- Port #: The port number.
- Direction: Direction of the frame through the port (I = In, O = Out).
- SOF: Start of frame.
- EOF: End of frame.
- Header: The 24 byte FC frame header.
- Payload Size: Size of the payload.
- Payload: The first 32 bytes of the FC frame payload.

Non-Wrapping Embedded Port Frame Log							
Count	Date/Time	Port #	Direction	SOF	EOF	Payload Size	
7	02/02/2004 10:48:20	13	O	f	t	0	
	Header: C0FFFFFFD 00FFFFFFD 00580000 01000000 00000001 00000001						
	Payload:						
6	02/02/2004 10:48:20	13	I	f	t	0	
	Header: C0FFFFFFD 00FFFFFFD 00580000 01000000 00000001 00000001						
	Payload:						
5	02/02/2004 10:48:20	13	O	f	n	8	
	Header: 03FFFFFFD 00FFFFFFD 22980000 01000000 00000001 00000000						
	Payload: 01000000 00FF0100						
4	02/02/2004 10:48:20	13	I	f	n	8	
	Header: 03FFFFFFD 00FFFFFFD 22980000 01000000 00000001 00000000						
	Payload: 01000000 00FF0100						

Figure 4-8 Viewing the Frame Log

Defining Filtering Settings

You can turn on filtering of Class F Frames and to choose which port to filter on. The settings take affect the way entries are added to the log, but do not affect the existing entries in the log. To define the settings, select the *Settings* button.

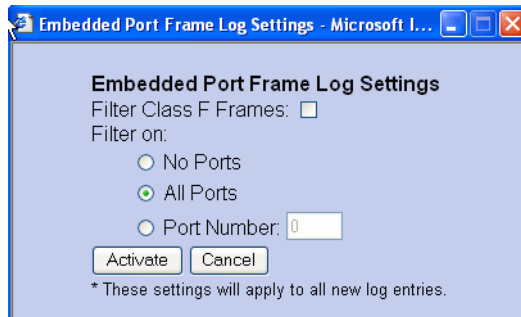


Figure 4-9 Setting Embedded Port Frame Filtering

Clearing Embedded Port Frame Log Entries

ATTENTION! Before clearing logs, make sure the logs are not needed for troubleshooting. Once a log is cleared, the data cannot be retrieved.

To clear the Embedded Frame Log, select *Monitor* and select the *Logs* tab and then select the *Clear Log* button. A message displays stating that the operation has been performed successfully.

Viewing All Logs

Select *Monitor* on the navigation panel. Select the *Logs* tab; the *Logs* tab view displays. Select the *All Logs* link. The All Logs listing displays in text format, as shown in [Figure 4-10](#). The log displays in a separate browser window. Close the browser window to close the log.

Event Log				
Date/Time	Error Code	Severity	Event Data	
4/26/04 4:38 pm	584	Major	17FF FFFF C3C8 0400 0AE7 1DFC FFFF FFFF FFFF FFFF FFFF	
4/26/04 4:38 pm	584	Major	0FFF FFFF B8C8 0400 0A67 DEC1 FFFF FFFF FFFF FFFF FFFF	
4/26/04 4:34 pm	422	Informational		
4/26/04 4:33 pm	417	Informational	3036 2E30 322E 3030 2031 3800 0000 0000 00	
4/26/04 4:33 pm	410	Informational	44	
4/26/04 4:33 pm	421	Informational	3036 2E30 322E 3030 2031 3800 0000 0000 00	
4/26/04 4:32 pm	423	Informational		
Open Trunking Re-Route Log				
Date/Time	Receive Port	Target Domain	Old Exit Port	New Exit Port
4/26/04 4:47 pm	15	27	0	1
4/26/04 4:43 pm	15	27	0	1
Link Incident Log				
Date/Time	Port	Link Incident Event		
4/26/04 4:38 pm	23	Not Operational primitive sequence (NOS) received.		
4/26/04 4:38 pm	15	Not Operational primitive sequence (NOS) received.		

Figure 4-10 All Logs View

The **All Logs** listing provides the ability to view (display) all of the content of the logs.

Clearing All Log Entries

ATTENTION! Before clearing information in all of the logs, make sure the logs are not needed for troubleshooting. Once the logs are cleared, the data cannot be retrieved.

To clear all logs' entries, select *Monitor* and select the *Logs* tab. Select the *Clear All Logs* button, next to the *All Logs* link. A message displays stating that the operation has been performed

SAN Management Logs

To open a log from a SAN management application main window, select the *Logs* option from the *Monitor* menu, then click (select) the desired log option.

Audit Log

To open the *Audit Log*, select the option from the *Monitor* and *Logs* menus. The log displays a history of user actions performed through the SAN management application. This information is useful for system administrators and users. For a log description, refer to the *SANavigator Software Release 4.0 User Manual* (621-000013).

Event Log

To open the *Event Log*, select the option from the *Monitor* and *Logs* menus. The log displays (Figure 4-11).

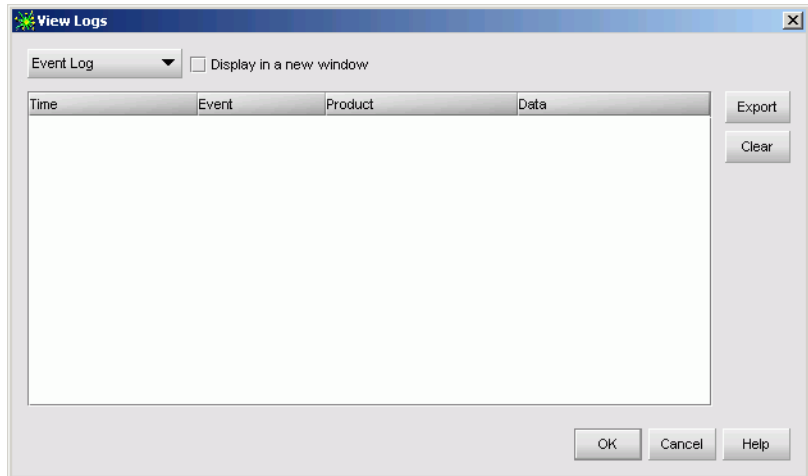


Figure 4-11 Event Log

The log displays SNMP trap events, client-server communication errors, and other problems recorded by the SAN management application. Information provided is generally intended for use by third-level support personnel to fault isolate significant problems. The log consists of the following columns:

- **Date/Time** - Date and time the event occurred.
- **Event** - Event number and brief description of the event. Include this information when reporting an event to customer support.
- **Product** - The product associated with the event and configured name or internet protocol (IP) address associated with the instance are displayed.
- **Data** - Additional event data for fault isolation. Include this information when fault isolating a call-home problem, or include the information when reporting an event to customer support.

Session Log

To open the *Session Log*, select the option from the *Monitor* and *Logs* menus. The log displays a session (login and logout) history for the SAN management application. This information is useful for system administrators and users. For a log description, refer to the *SANavigator Software Release 4.0 User Manual* (621-000013).

Product Status Log

To open the *Product Status Log*, select the option from the *Monitor* and *Logs* menus. The log displays ([Figure 4-12](#)).

Time	Network Address	Previous Status	New Status
2003/09/04 09:21:57	172.31.1.11	Unknown	OutOfBand Online
2003/09/04 09:21:33	172.31.1.11	Unknown	OutOfBand Offline
2003/09/04 09:20:54	172.31.1.32	Unknown	OutOfBand Online
2003/09/04 09:19:15	172.31.1.32	Unknown	OutOfBand Offline
2003/09/04 09:12:41	172.31.1.32	Unknown	OutOfBand Online
2003/09/04 09:07:29	172.31.1.32	Unknown	OutOfBand Offline
2003/09/04 08:59:53	172.31.1.32	Unknown	OutOfBand Online
2003/09/04 08:58:17	172.31.1.32	Unknown	OutOfBand Offline
2003/09/04 08:54:57	172.31.1.32	Unknown	OutOfBand Online
2003/09/04 08:53:23	172.31.1.32	Unknown	OutOfBand Offline
2003/09/04 08:51:59	172.31.1.32	Unknown	OutOfBand Online
2003/09/04 08:50:32	172.31.1.11	Unknown	OutOfBand Online
2003/09/04 08:50:06	172.31.1.11	Unknown	OutOfBand Offline
2003/09/04 08:49:27	172.31.1.32	Unknown	OutOfBand Offline

Figure 4-12 Product Status Log

The log reflects the previous and current status of the switch, and indicates the instance of a Sphereon 4500 Element Manager application that should be opened to investigate a problem. The information is useful to maintenance personnel for fault isolation and repair verification. The log consists of the following columns:

- **Date/Time** - Date and time the switch status change occurred.
- **Network Address** - IP address or configured name of the switch. This address or name corresponds to the address or name displayed under the product icon at the physical map.
- **Previous Status** - Status of the switch prior to the reported status change (*Operational*, *Degraded*, *Failed*, *OutOfBand Online*, or *Unknown*). An *Unknown* status indicates the SAN management application cannot communicate with the switch.
- **New Status** - Status of the switch after to the reported status change (*Operational*, *Degraded*, *Failed*, *OutOfBand Online*, or *Unknown*).

Fabric Log

To open the *Fabric Log*, select the option from the *Monitor* and *Logs* menus. The log reflects the time and nature of changes made to a managed fabric. This information is useful for system administrators and users. For a log description, refer to the *SANavigator Software Release 4.0 User Manual* (621-000013).

Element Manager Logs

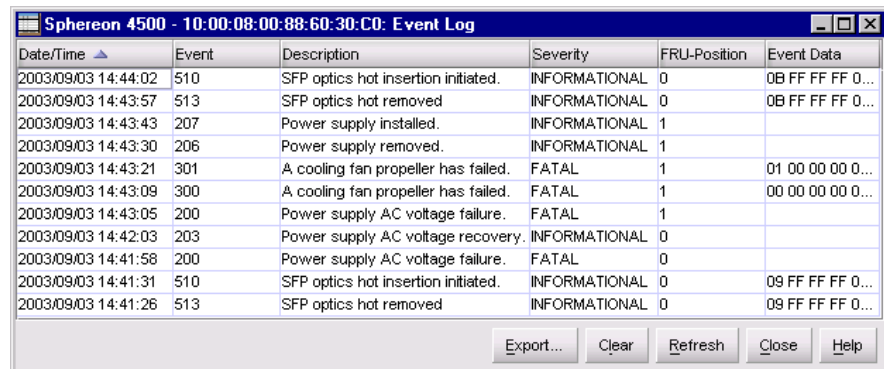
To open a log from the Element Manager application, select the *Logs* menu at any view, then click (select) the desired log option.

Sphereon 4500 Audit Log

To open the *Sphereon 4500 Audit Log*, select the *Audit Log* option from the *Logs* menu at the *Hardware View*, *Port List View*, *Node List View*, *Performance View*, or *FRU List View*. The log displays a history of user actions performed through the Element Manager application or a simple network management protocol (SNMP) management workstation. This information is useful for system administrators and users. For a log description and an explanation of button functions, refer to the *McDATA Sphereon 4500 Fabric Switch Element Manager User Manual* (620-000175).

Sphereon 4500 Event Log

To open the *Sphereon 4500 Event Log*, select the *Event Log* option from the *Logs* menu at the *Hardware View*, *Port List View*, *Node List View*, *Performance View*, or *FRU List View*. The log displays (Figure 4-13).



Date/Time	Event	Description	Severity	FRU-Position	Event Data
2003/09/03 14:44:02	510	SFP optics hot insertion initiated.	INFORMATIONAL	0	0B FF FF FF 0...
2003/09/03 14:43:57	513	SFP optics hot removed	INFORMATIONAL	0	0B FF FF FF 0...
2003/09/03 14:43:43	207	Power supply installed.	INFORMATIONAL	1	
2003/09/03 14:43:30	206	Power supply removed.	INFORMATIONAL	1	
2003/09/03 14:43:21	301	A cooling fan propeller has failed.	FATAL	1	01 00 00 00 0...
2003/09/03 14:43:09	300	A cooling fan propeller has failed.	FATAL	1	00 00 00 00 0...
2003/09/03 14:43:05	200	Power supply AC voltage failure.	FATAL	1	
2003/09/03 14:42:03	203	Power supply AC voltage recovery.	INFORMATIONAL	0	
2003/09/03 14:41:58	200	Power supply AC voltage failure.	FATAL	0	
2003/09/03 14:41:31	510	SFP optics hot insertion initiated.	INFORMATIONAL	0	09 FF FF FF 0...
2003/09/03 14:41:26	513	SFP optics hot removed	INFORMATIONAL	0	09 FF FF FF 0...

Figure 4-13 Sphereon 4500 Event Log

The log displays a history of switch events, such as degraded operation, FRU failures, FRU removals and replacements, port problems, Fibre Channel link incidents, and management server-to-switch communication problems. The information is useful to maintenance personnel for fault isolation and repair verification.

The log consists of the following columns:

- **Date/Time** - Date and time the event occurred.
- **Event** - Three-digit code that describes the event. Event codes are listed and described in [Appendix B: Event Code Tables](#) on page B-1.
- **Description** - Brief description of the event.
- **Severity** - Severity of the event (*Informational, Minor, Major, or Fatal*).
- **FRU-Position** - Acronym representing the FRU type, followed by a number representing the FRU chassis position. Acronyms are:
 - **CTP** - Control processor (CTP) card. The chassis slot is **0**. The CTP card is not a FRU.
 - **PWR** - Power supply. Chassis slots for redundant power supplies are **0** and **1**.

Three cooling fans are integrated in each power supply. Cooling fans are not FRUs. A failed cooling fan requires replacement of the power supply.
- **Event Data** - Up to 32 bytes of supplementary information (if available) in hexadecimal format. Event data is described in [Appendix B: Event Code Tables](#) on page B-1.

To ensure recently-created events appear in the log, periodically refresh the log display. This is important when inspecting the log to verify a repair procedure. To refresh the log, click *Refresh*.

Hardware Log To open the *Hardware Log*, select the *Hardware Log* option from the *Logs* menu at the *Hardware View*, *Port List View*, *Node List View*, *Performance View*, or *FRU List View*. The log displays ([Figure 4-14](#)).

Date/Time	FRU	Position	Action	Part Number	Serial Number
2003/09/03 14:48:21	Power	1	Inserted		
2003/09/03 14:48:05	Power	1	Removed		

Figure 4-14 Hardware Log

The log displays a history of FRU removals and replacements (insertions) for the switch. The information is useful to maintenance personnel for fault isolation and repair verification. The log consists of the following columns:

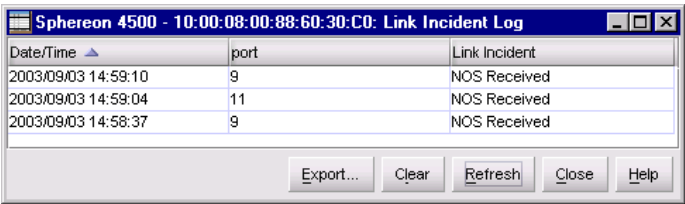
- **Date/Time** - Date and time the FRU was inserted or removed.
- **FRU** - Acronym representing the FRU type. FRU acronyms are:
 - **CTP** - Control processor card. The CTP card is not a FRU. A failed CTP card requires replacement of the switch.
 - **PWR** - Power supply.

Three cooling fans are integrated in each power supply. Cooling fans are not FRUs. A failed cooling fan requires replacement of the power supply.

- **Position** - Number representing the FRU chassis position. The chassis (slot) position for a nonredundant CTP card is **0**. Chassis slots for redundant power supplies are **0** and **1**.
- **Action** - Action performed (*Inserted* or *Removed*).
- **Part Number** - Part number of the inserted or removed FRU.
- **Serial Number** - Serial number of the inserted or removed FRU.

Link Incident Log

To open the *Link Incident Log*, select the *Link Incident Log* option from the *Logs* menu at the *Hardware View*, *Port List View*, *Node List View*, *Performance View*, or *FRU List View*. The log displays (Figure 4-15).



Date/Time	port	Link Incident
2003/09/03 14:59:10	9	NOS Received
2003/09/03 14:59:04	11	NOS Received
2003/09/03 14:58:37	9	NOS Received

Figure 4-15 Link Incident Log

The log displays a history of Fibre Channel link incidents (with associated port numbers) for the switch. The information is useful to maintenance personnel for isolating port problems and repair verification. The log consists of the following columns:

- **Date/Time** - Date and time the link incident occurred.
- **Port** - Port number (0 through 23) that reported the link incident.
- **Link Incident** - Brief description of the link incident. Problem descriptions include:
 - Implicit incident.
 - Bit-error threshold exceeded.
 - Link failure - loss of signal or loss of synchronization.
 - Link failure - not-operational primitive sequence (NOS) received.
 - Link failure - primitive sequence timeout.
 - Link failure - invalid primitive sequence received for current link state.

Refer to [MAP 0600: Port Failure and Link Incident Analysis](#) on page 3-74 for corrective actions in response to these link incident messages.

Threshold Alert Log

To open the *Threshold Alert Log*, select the *Threshold Alert Log* option from the *Logs* menu at the *Hardware View*, *Port List View*, *Node List View*, *Performance View*, or *FRU List View*. The log displays (Figure 4-16).

Date/Time	Name	Port	Type	Utilization %	Interval
2003/09/04 12:45:41	Port 1 50%	1	Receive And ...	50	5
2003/09/04 12:45:41	Port 3 75%	3	Receive And ...	75	5
2003/09/04 12:45:41	Port 5 & 7 70%	5	Receive And ...	70	5
2003/09/04 12:45:41	Port 5 & 7 70%	7	Receive And ...	70	5
2003/09/04 12:44:41	Testing	1	Receive And ...	50	5
2003/09/04 12:44:41	Testing	3	Receive And ...	50	5
2003/09/04 12:44:41	Testing	5	Receive And ...	50	5
2003/09/04 12:44:41	Testing	7	Receive And ...	50	5
2003/09/04 12:44:41	75%	1	Receive And ...	75	5
2003/09/04 12:44:41	75%	3	Receive And ...	75	5
2003/09/04 12:44:41	75%	5	Receive And ...	75	5
2003/09/04 12:44:41	75%	7	Receive And ...	75	5
2003/09/04 12:40:45	Port 1 50%	1	Receive And ...	50	5

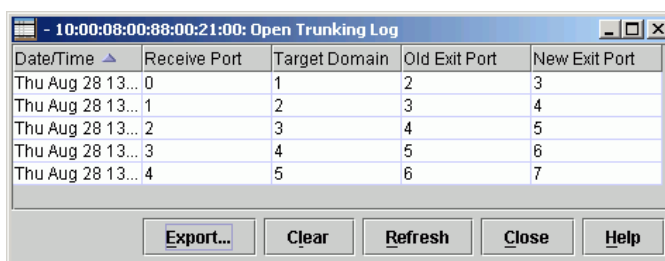
Figure 4-16 Threshold Alert Log

The log displays a history of threshold alert notifications. The log consists of the following columns:

- **Date/Time** - Date and time the alert occurred.
- **Name** - Name for the alert as configured through the *Configure Threshold Alerts* dialog box.
- **Port** - Port number where the alert occurred.
- **Type** - Type of alert: transmit (*Tx*) or receive (*Rx*).
- **Utilization %** - Percent usage of traffic capacity. This setting constitutes the threshold value and is configured through the *Configure Threshold Alerts* dialog box. For example, a value of 25 means that threshold occurs when throughput reaches 25 percent of the port's capacity.
- **Interval** - Time interval during which the throughput is measured and an alert can generate. This is set through the *Configure Threshold Alerts* dialog box.

Open Trunking Log

To open the *Open Trunking Log*, select the *Open Trunking Log* option from the *Logs* menu at the *Hardware View*, *Port List View*, *Node List View*, *Performance View*, or *FRU List View*. The log displays (Figure 4-17).



The screenshot shows a window titled "- 10:00:08:00:88:00:21:00: Open Trunking Log". It contains a table with the following data:

Date/Time	Receive Port	Target Domain	Old Exit Port	New Exit Port
Thu Aug 28 13:00:08	0	1	2	3
Thu Aug 28 13:00:11	1	2	3	4
Thu Aug 28 13:00:12	2	3	4	5
Thu Aug 28 13:00:13	3	4	5	6
Thu Aug 28 13:00:14	4	5	6	7

Below the table are buttons for **Export...**, **Clear**, **Refresh**, **Close**, and **Help**.

Figure 4-17 Open Trunking Log

The log displays ISL congestion events that cause Fibre Channel traffic to be routed through an alternate ISL. Entries reflect the traffic re-route status at the managed switch. The log consists of the following columns:

- **Date/Time** - Date and time the re-route action occurred.
- **Receive Port** - The switch port number (decimal) used for receiving Fibre Channel traffic after the re-route action.
- **Target Domain** - The domain ID (decimal) of the target device to which Fibre Channel traffic from the switch was rerouted.

- **Old Exit Port** - The switch port number (decimal) used for transmitting Fibre Channel traffic before the re-route action.
- **New Exit Port** - The switch port number (decimal) used for transmitting Fibre Channel traffic after the re-route action.

Obtain Port Diagnostic Information

Fibre Channel port diagnostic information can be obtained by:

- Inspecting port LEDs at the switch front panel or emulated port LEDs at the management server’s *Hardware View*.
- Inspecting parameters at the SANpilot interface.
- Inspecting parameters at the management server (Sphereon 4500 Element Manager application).

Port LEDs

To obtain port operational information, inspect port LEDs at the switch front panel or emulated port LEDs at the management server’s *Hardware View*. Amber and blue/green LEDs adjacent to each port indicate operational status as described in [Table 4-1](#).

Table 4-1 Port Operational States

Port State	Blue/Green LED	Amber LED	Alert Symbol	Description
Online	On or Blinking	Off	None	<p>An attached device is connected to the switch and ready to communicate, or is communicating through the switch with other attached devices.</p> <p>If the port remains online at 1.0625 Gbps, the blue/green LED illuminates green. If the port remains online at 2.125 Gbps, the blue/green LED illuminates blue.</p> <p>At the switch, the blue/green LED blinks green when there is Fibre Channel traffic through the port at 1.0625 Gbps. At the switch, the blue/green LED blinks blue when there is Fibre Channel traffic through the port at 12.125 Gbps.</p>
Offline	Off	Off	None	The port is blocked and transmitting the offline sequence (OLS) to the attached device.
	Off	Off	Yellow Triangle	The port is unblocked and receiving the OLS, indicating the attached device is offline.

Table 4-1 Port Operational States (continued)

Port State	Blue/Green LED	Amber LED	Alert Symbol	Description
Beaconing	Off, On, or Blinking	Blinking	Yellow Triangle	The port is beaconing. The amber port LED blinks once every two seconds to enable users to locate the port.
Invalid Attachment	On	Off	Yellow Triangle	The port has an invalid attachment. The reason appears in the <i>Reason</i> field at the <i>Port Properties</i> dialog box.
Link Incident	Off	Off	Yellow Triangle	A link incident occurred. The alert symbol appears at the <i>Hardware View</i> and <i>Port List View</i> .
Link Reset	Off	Off	Yellow Triangle	The switch and attached device are performing a link reset operation to recover the link connection. This is a transient state that should not persist.
No Light	Off	Off	None	No signal (light) is received at the switch port. This is a normal condition when there is no cable attached to the port or when the attached device is powered off.
Inactive	On	Off	Yellow Triangle	The port is inactive. The reason appears in the <i>Reason</i> field at the <i>Port Properties</i> dialog box.
Not Installed	Off	Off	None	An optical transceiver is not installed in the switch port.
Not Operational	Off	Off	Yellow Triangle	The port is receiving the not operational sequence (NOS) from an attached device.
Port Failure	Off	On	Red and Yellow Blinking Diamond	The port failed and requires service.
Segmented E_Port	On	Off	Yellow Triangle	The E_Port is segmented, preventing two connected switches from joining and forming a multiswitch fabric. The reason appears in the <i>Reason</i> field of the <i>Port Properties</i> dialog box.
Testing	Off	Blinking	Yellow Triangle	The port is performing an internal loopback test.
	On	Blinking	Yellow Triangle	The port is performing an external loopback test.

SANpilot Interface

To obtain port operational information at the SANpilot interface, inspect parameters at the:

- *Monitor Panel - Port List* page.
- *Monitor Panel - Port Stats* page.
- *View* panel - *Port Properties* page.

Port List Page

When the SANpilot interface opens, the *View* panel appears as the default panel. At the *View* panel, select the *Monitor* option at the left side of the panel. The *Monitor* panel opens with the *Port List* page displayed (Figure 4-18).

Port #	Name	Block Configuration	State	Type
0		Unblocked	Offline	Gx Port
1		Unblocked	Offline	Gx Port
2		Unblocked	Offline	Gx Port
3		Unblocked	Offline	Gx Port
4		Unblocked	Offline	Gx Port
5		Unblocked	Offline	Gx Port
6		Unblocked	Offline	Gx Port
7		Unblocked	Offline	Gx Port
8		Unblocked	Offline	Gx Port
9		Unblocked	Offline	Gx Port
10		Unblocked	Offline	Gx Port
11		Unblocked	Offline	Gx Port

Figure 4-18 Monitor Panel (Port List Page)

A row of information for each port (0 through 23 inclusive) appears. Each row consists of the following columns:

- **Port #** - Switch port number.
- **Name** - Port name of 24 alphanumeric characters or less. The name typically characterizes the device or fabric element to which the port is attached.
- **Block Configuration** - Indicates if a port is blocked or unblocked. Blocking a port prevents the attached devices or fabric element from communicating. A blocked port continuously transmits the offline sequence (OLS).
- **State** - Port state (*Online*, *Offline*, *Not Installed*, *Inactive*, *Invalid Attachment*, *Link Reset*, *No Light*, *Not Operational*, *Port Failure*, *Segmented E_Port*, or *Testing*).

- **Type** - Configured port type. Settings are:
 - Generic mixed port (GX_Port). This setting also configures a port as a generic loop port (GL_Port).
 - Fabric mixed port (FX_Port). This setting also configures a port as a fabric loop port (FL_Port).
 - Generic port (G_Port).
 - Fabric port (F_Port).
 - Expansion port (E_Port).

Port Stats Page

When the SANpilot interface opens, the *View* panel appears as the default panel. At the *View* panel, select the *Monitor* option at the left side of the panel. The *Monitor* panel opens with the *Port List* page displayed. Click the *Port Stats* tab. The *Monitor* panel displays with the *Port Stats* page selected (Figure 4-19).

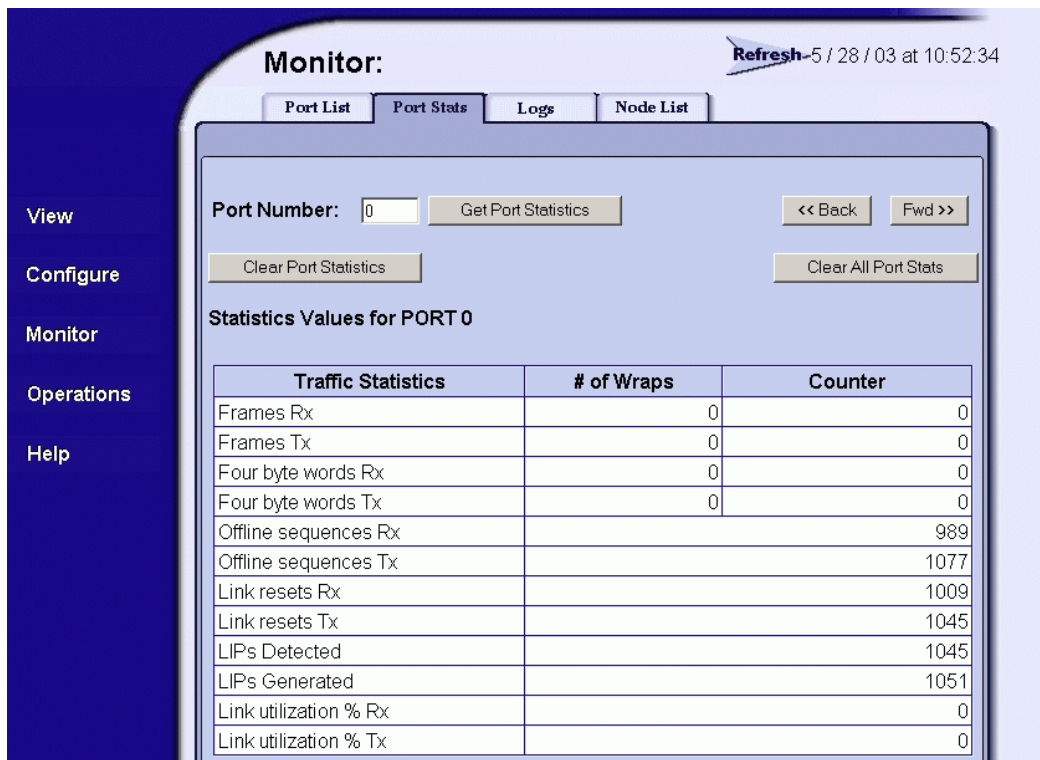


Figure 4-19 Monitor Panel (Port Stats Page)

Troubleshooting Tip for Port Statistics

As a general rule, you should clear all the counters by selecting *Clear Port Stats* or *Clear All Port Stats* after you have resolved a problem. When troubleshooting, keep track of the time interval when errors accumulate to judge the presence and severity of a problem. (There is a link recovery hierarchy implemented in Fibre Channel to handle some level of “expected anomalies”.) For troubleshooting purposes, you want to focus on when the errors, as displayed in the *Counter* column, increment very quickly.

Parts of Statistics Tables

The tables of statistics contain the following columns:

- **Statistics** - the type of statistic being tracked.
- **# of Wraps** - times the *Counter* value wraps, for statistics that grow rapidly. The maximum value that either the *Counter* or the *# of Wraps* can hold is 2^{32} , or 4,294,967,296. Each time the *Counter* field reaches the maximum value of 2^{32} , the wrap count is incremented by 1.
- **Counter** - the number of instances of the tracked item recorded since system initialization or the last time the counters were cleared.

Traffic Transmit and Receive Statistics

The Traffic Statistics include these transmit and receive values.

- **Frames Rx** - The number of frames that the port has received.
- **Frames Tx** - The number of frames that the port has transmitted.
- **Four byte words Rx** - The number of words that the port has received.
- **Four byte words Tx** - The number of words that the port has transmitted.
- **Offline sequences Rx** - The number of offline sequences (OLS) received by this port.
- **Offline sequences Tx** - The number of offline sequences (OLS) transmitted by this port.
- **Link resets Rx** - The number of link reset protocol frames received by this port from the attached N_Port.
- **Link resets Tx** - The number of link reset protocol frames transmitted by this port to the attached N_Port.

- **Link utilization % Rx** - The current link utilization for the port expressed as a percentage. On 1 Gbps links, ports can transmit or receive data at 100 MB per second. On 2 Gbps links, ports can transmit or receive data at 200 MB per second. Link utilization is calculated over one-second intervals.
- **Link utilization % Tx** - The current link utilization for the port expressed as a percentage. On 1 Gbps links, ports can transmit or receive data at 100 MB per second. On 2 Gbps links, ports can transmit or receive data at 200 MB per second. Link utilization is calculated over one-second intervals.

Other statistics are also shown:

- **LIPs Detected** - A loop initialization primitive was detected, which means the loop was completed.
- **LIPs Generated** - A loop initialization primitive was created to initialize a loop.

Error Statistics

The Error Statistics include these transmit and receive values:

- **Link failures** - The number of link failures recorded because a not operational sequence (NOS), protocol timeout, or port failure was detected.
- **Sync losses** - The number of loss-of-synchronizations detected because an attached device was reset or disconnected from the port.
- **Signal losses** - The number of loss-of-signal errors detected because the attached device was reset or disconnected from the port.
- **Primitive sequence errors** - The number of primitive sequence protocol errors received from an attached device, which indicates a Fibre Channel link-level protocol violation.
- **Discarded frames** - A received frame could not be routed and was discarded because the frame timed out due to an insufficient buffer-to-buffer credit, or the destination device was not logged into the product.
- **Invalid transmission words** - The number of invalid transmission words from an attached device. This indicates that a frame or primitive sequence arrived at the port corrupted.

- **CRC errors** - A received frame failed a cyclic redundancy check (CRC) validation, indicating the frame arrived at the port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure, a bad fiber-optic cable, or a poor cable connection.
- **Delimiter errors** - The number of times that the switch detected an unrecognized start-of-frame (SOF), an unrecognized end-of-frame (EOF) delimiter, or an invalid class of service. This indicates that the frame arrived at the switch's port corrupted. This corruption can be due to plugging/unplugging the link, bad optics at either end of the cable, bad cable, or dirty or poor connections. Moving the connection around or replacing cables can isolate the problem.
- **Address ID errors** - A received frame had an unavailable or invalid Fibre Channel destination address, or an invalid Fibre Channel source address. This typically indicates the destination device is unavailable.
- **Frames too short** - A received frame exceeded the Fibre Channel frame maximum size or was less than the Fibre Channel minimum size, indicating the frame arrived at the switch's port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.

Class 2 Statistics

The Class 2 Statistics include these transmit and receive values:

- **Received Frames** - The number of Class 2 frames received by this F_Port from its attached N_Port.
- **Transmitted Frames** - The number of Class 2 frames transmitted by this F_Port to its attached N_Port.
- **4-byte words Rx** - The number of Class 2, 4-byte words received by the port.
- **4-byte words Tx** - The number of Class 2, 4-byte words transmitted by the port.
- **Busied Frames** - The number of F_BSY frames generated by this F_Port against Class 2 frames.
- **Rejected Frames** - The number of F_RJT frames generated by this F_Port against Class 2 frames.

Class 3 Statistics

The Class 3 Statistics include these transmit and receive values:

- **Received Frames** - The number of Class 3 frames received by the F_Port from its attached N_Port.
- **Transmitted Frames** - The number of Class 3 frames transmitted by this F_Port to its attached N_Port.
- **Discarded Frames** - The number of Class 3 frames discarded (including multicast frames with bad Domain IDs).
- **4-byte words Rx** - The number of Class 3, 4-byte words received by the port.
- **4-byte words Tx** - The number of Class 3, 4-byte words transmitted by the port.

Open Trunking Statistics

The Open Trunking Statistics include these transmit and receive values:

- **Flows rerouted to ISL** - The number of Fibre Channel traffic flows that were rerouted to this ISL from another ISL due to congestion. (This value increments only if the OpenTrunking feature is installed.)
- **Flows rerouted from ISL** - The number of Fibre Channel traffic flows that were rerouted from this ISL to another ISL due to congestion. (This value increments only if the OpenTrunking feature is install

Port Properties Page

When the SANpilot interface opens, the *View* panel appears as the default panel. At the *View* panel, click the *Port Properties* tab. The *View* panel displays with the *Port Properties* page selected ([Figure 4-20](#) on page 4-29).

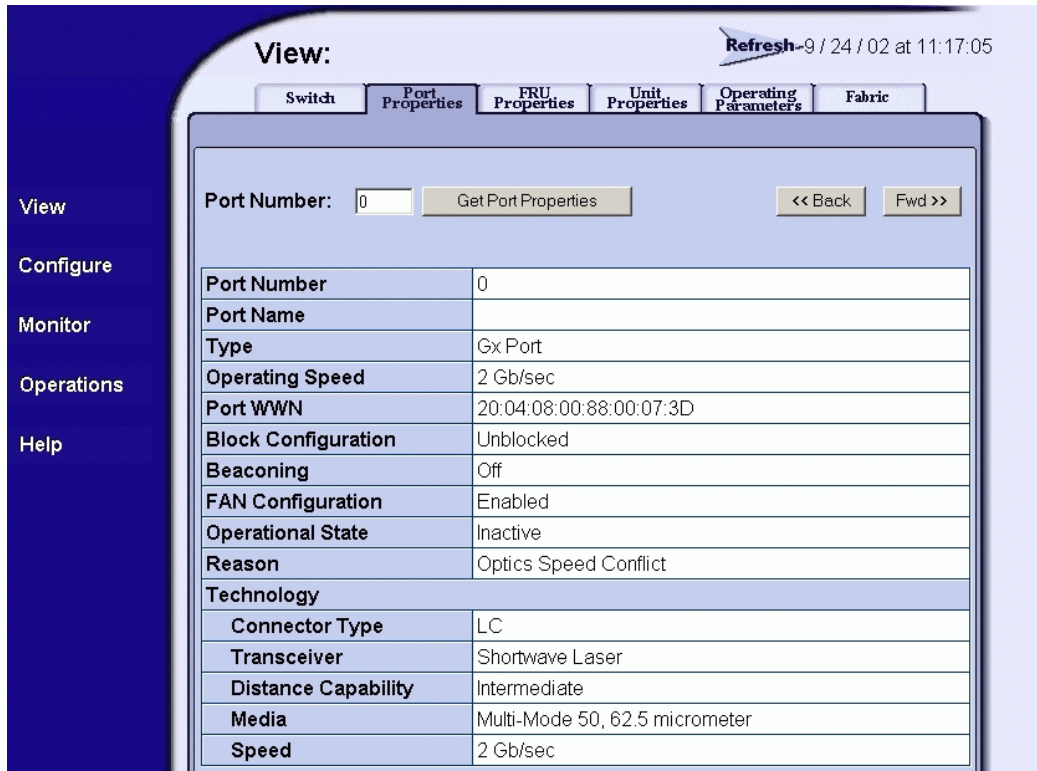


Figure 4-20 View Panel (Port Properties Page)

The *Port Properties* page displays information for one port. Values update only when the page opens for a selected port or the user selects *Get Port Properties*. The page defaults to port 0. Increment or decrement the port number displayed (0 through 23 inclusive) by clicking *Fwd>>* or *<<Back*. The page provides the following information:

- **Port Number** - Switch port number.
- **Port Name** - User-defined name or description for the port.
- **Type** - Port type (*GX_Port*, *FX_Port*, *G_Port*, *F_Port*, or *E_Port*).
- **Operating Speed** - Operating speed (*Not Established*, *1 Gbps*, or *2 Gbps*).
- **Port WWN** - Fibre Channel world wide name (WWN) for the port.

- **Block Configuration** - User-configured state for the port (*Blocked* or *Unblocked*).
- **Beaconing** - User-specified for the port (*On* or *Off*).
- **FAN Configuration** - User-configured state for fabric address notification (FAN) configuration (*Enabled* or *Disabled*).
- **Operational State** - Port state (*Online*, *Offline*, *Not Installed*, *Inactive*, *Invalid Attachment*, *Link Reset*, *No Light*, *Not Operational*, *Port Failure*, *Segmented E_Port*, or *Testing*).
- **Reason** - A summary appears describing the reason if the port state is *Segmented E_Port*, *Invalid Attachment*, or *Inactive*. For any other port state, the reason is *N/A*.
- **Technology** - Information specific to the installed optical transceiver, including connector type, transceiver optics, data transmission distance, optical media (cable type), and transmission speed.

Management Server

To obtain port operational information at the management server (Element Manager application), inspect parameters at the:

- *Port List View*.
- *Performance View*.
- *Port Properties* dialog box.
- *Port Technology* dialog box.

Port List View

At the management server, click the *Port List* tab. The *Port List View* displays (Figure 4-21). A row of information for each port (0 through 23 inclusive) appears. Each row consists of the following columns:

- **Name** - Port name configured through the *Configure Ports* dialog box.
- **Block Config** - Indicates if a port is blocked or unblocked. Blocking a port prevents the attached devices or fabric element from communicating. A blocked port continuously transmits the OLS.
- **State** - Port state (*Online*, *Offline*, *Not Installed*, *Inactive*, *Invalid Attachment*, *Link Reset*, *No Light*, *Not Operational*, *Port Failure*, *Segmented E_Port*, or *Testing*).

MCDATA Sphereon 4500 : 4500-112						
Product Configure Logs Maintenance Help						
Hardware Port List Node List Performance FRU List						
Port #	Name	Block Config	State	Type	Operating Speed	Alert
0		Unblocked	No Light	GX_Port	Not Established	
1		Unblocked	Online	F_Port	1 Gig	▲
2		Unblocked	No Light	GX_Port	Not Established	
3		Unblocked	Online	F_Port	1 Gig	▲
4		Unblocked	No Light	GX_Port	Not Established	
5		Unblocked	Online	F_Port	1 Gig	▲
6		Unblocked	No Light	GX_Port	Not Established	
7		Unblocked	Online	F_Port	1 Gig	▲
8		Unblocked	No Light	GX_Port	Not Established	
9		Unblocked	Online	E_Port	1 Gig	▲
10		Unblocked	No Light	GX_Port	Not Established	
11		Unblocked	Online	E_Port	2 Gig	▲
12		Unblocked	No Light	GX_Port	Not Established	
13		Unblocked	No Light	GX_Port	Not Established	
14		Unblocked	No Light	GX_Port	Not Established	
15		Unblocked	No Light	GX_Port	Not Established	
16		Unblocked	No Light	GX_Port	Not Established	
17		Unblocked	No Light	GX_Port	Not Established	
18		Unblocked	No Light	GX_Port	Not Established	
19		Unblocked	No Light	GX_Port	Not Established	
20		Unblocked	No Light	GX_Port	Not Established	
21		Unblocked	No Light	GX_Port	Not Established	
22		Unblocked	No Light	GX_Port	Not Established	
23		Unblocked	No Light	GX_Port	Not Established	

Figure 4-21 Port List View

- **Type** - Port type (*GX_Port*, *FX_Port*, *G_Port*, *F_Port*, or *E_Port*).
- **Operating Speed** - Operating speed (*Not Established*, *1 Gbps*, or *2 Gbps*).
- **Alert** - If link incident (LIN) alerts are configured for the port through the *Configure Ports* dialog box, a yellow triangle appears in the column when a link incident occurs. A yellow triangle also appears if beaconing is enabled for the port. A red and yellow diamond appears if the port fails.

Click anywhere in the port row to open the *Port Properties* dialog box (Figure 4-23 on page 4-36). Right-click anywhere in the port row to open a pop-up menu to:

- Open the *Port Properties* dialog box (Figure 4-23 on page 4-36).
- Open the *Port Technology* dialog box (Figure 4-24 on page 4-37).

- Block or unblock the port.
- Enable or disable port beaconing.
- Perform port diagnostics.
- Clear link incident alerts.
- Reset the port.
- Enable or disable port binding.
- Clear threshold alerts.

Performance View

At the management server, click the *Performance* tab. The *Performance View* displays (Figure 4-22). The view provides statistical information about port performance that is useful to maintenance personnel for isolating port problems.

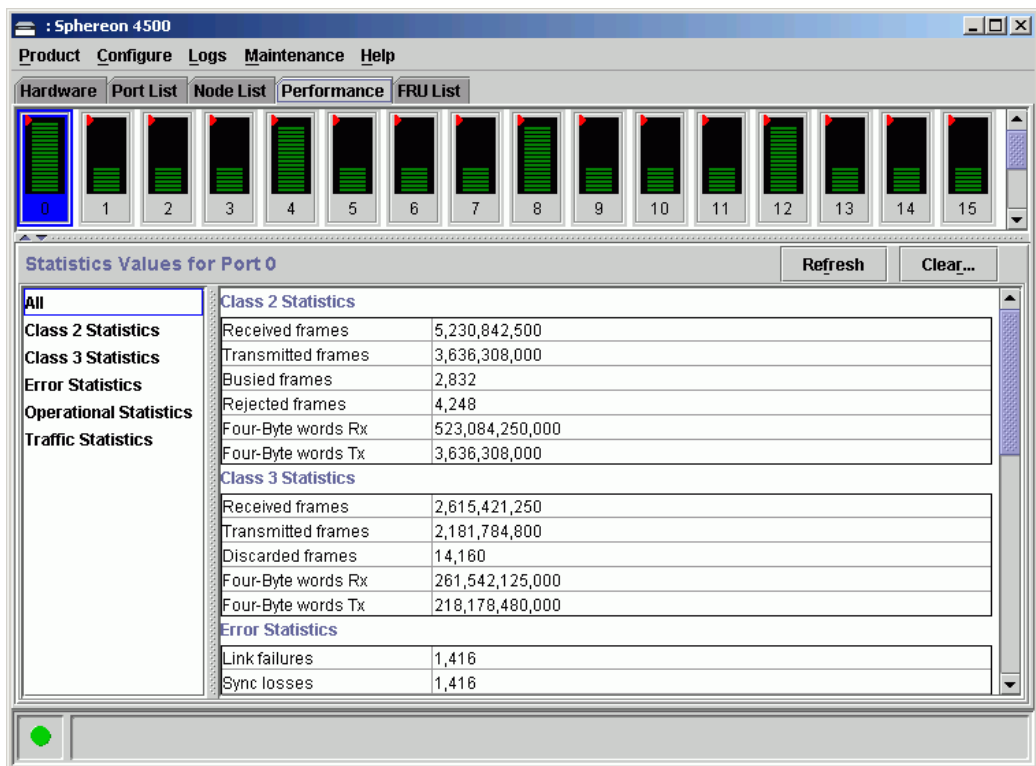


Figure 4-22 Performance View

Each port bar graph in the upper portion of the view displays the instantaneous transmit or receive activity level for the port, and is updated every five seconds. The relative value displayed is the greater of either the transmit or receive activity (whichever value is greatest when sampled).

Each port graph has 20 green-bar level indicators corresponding to 5% of the maximum throughput for the port (either transmit or receive). If any activity is detected for a port, at least one green bar appears. A red indicator on each port bar graph (high-water mark)

remains at the highest level the graph has reached since the port was set online. The indicator does not appear if the port is offline, and is reset to the bottom of the graph if the port detects a loss of light.

When the mouse cursor is passed over a port bar graph (flyover), the graph highlights with a blue border and an information pop-up displays the port operational state or WWN of the attached device. Click a port bar graph to display statistics values for the port.

Right-click a port bar graph to open a pop-up menu to:

- Open the *Port Properties* dialog box ([Figure 4-23](#) on page 4-36).
- Open the *Port Technology* dialog box ([Figure 4-24](#) on page 4-37).
- Block or unblock the port.
- Enable or disable port beaconing.
- Perform port diagnostics.
- Clear link incident alerts.
- Reset the port.
- Enable or disable port binding.
- Clear threshold alerts.

The page displays the following tables of cumulative port statistics and error count values for a selected port:

- **Class 2 statistics** - These entries provide information about Class 2 traffic, including:
 - Class 2 frames received and transmitted.
 - Four-byte words received and transmitted.
 - Busied and rejected frames.

- **Class 3 statistics** - These entries provide information about Class 3 traffic, including:
 - Class 3 frames received and transmitted.
 - Four-byte words received and transmitted.
 - Discarded frames.
- **Error statistics** - The *Performance View* displays the following error statistics for the port:
 - **Link failures** - Link failures are recorded in response to an NOS, protocol timeout, or port failure. At the *Hardware View*, a yellow triangle appears to indicate a link incident, or a blinking red and yellow diamond appears to indicate a port failure.
 - **Sync losses** - Synchronization losses are detected because an attached device was reset or disconnected from the port. At the *Hardware View*, a yellow triangle appears to indicate a link incident.
 - **Signal losses** - Signal losses are detected because an attached device was reset or disconnected from the port. At the *Hardware View*, a yellow triangle appears to indicate a link incident.
 - **Primitive sequence errors** - Incorrect primitive sequences are received from an attached device, indicating Fibre Channel link-level protocol violations. At the *Hardware View*, a yellow triangle appears to indicate a link incident.
 - **Discarded frames** - Received frames could not be routed and were discarded because the frame timed out (insufficient buffer-to-buffer credit) or the destination device was not logged into the switch.
 - **Invalid transmission words** - Several transmission words were received with encoding errors, indicating an attached device is not operating in conformance with the Fibre Channel specification.
 - **CRC errors** - Received frames failed CRC validation, indicating the frames arrived at the switch port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.

- **Delimiter errors** - Received frames had frame delimiter errors, indicating the frame arrived at the switch port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.
- **Address ID errors** - Received frames had unavailable or invalid Fibre Channel destination addresses, or invalid Fibre Channel source addresses. This typically indicates the destination device is unavailable.
- **Frames too short** - Received frames were less than the Fibre Channel minimum size, indicating the frame arrived at the switch port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.
- **Operational statistics** - These entries provide information about port operation, including:
 - Offline sequences received and transmitted.
 - Link resets received and transmitted.
 - LIPs generated and detected.
- **Traffic statistics** - These entries provide information about port traffic, including:
 - Percent link utilization (receive and transmit).
 - Fibre Channel frames received and transmitted.
 - Four-byte words received and transmitted.
 - Flows rerouted to and from ISLs.

Port Properties Dialog Box

To open the *Port Properties* dialog box ([Figure 4-23](#) on page 4-36), double-click a port graphic at the *Hardware View* or a port row at the *Port List View*. The dialog box provides the following information:

- **Port Number** - Switch port number (0 through 23 inclusive).
- **Port Name** - Port name configured through the *Configure Ports* dialog box.
- **Type** - Port type (*GX_Port*, *FX_Port*, *G_Port*, *F_Port*, or *E_Port*).
- **Operating Speed** - operating speed (*Not Established*, *1 Gbps*, or *2 Gbps*).

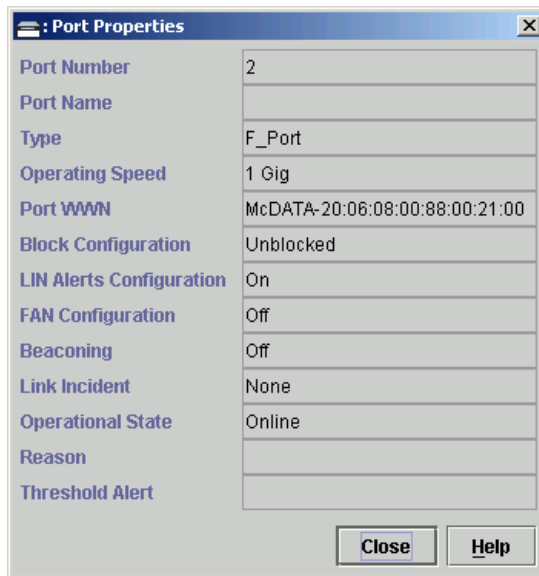


Figure 4-23 Port Properties Dialog Box

- **Port WWN** - Fibre Channel WWN for the port.
- **Block Configuration** - User-configured state for the port (*Blocked* or *Unblocked*).
- **LIN Alerts Configuration** - User-configured state for LIN alerts configuration (*On* or *Off*).
- **FAN Configuration** - User-configured state for FAN configuration (*Enabled* or *Disabled*).
- **Beaconing** - User-specified for the port (*On* or *Off*). When beaconing is enabled, a yellow triangle appears adjacent to the status field.
- **Link Incident** - If no link incidents are recorded, *None* appears in the status field. If a link incident is recorded, a summary appears describing the incident, and a yellow triangle appears adjacent to the status field. Valid summaries are:
 - Implicit incident.
 - Bit-error threshold exceeded.
 - Link failure - loss of signal or loss of synchronization.

- Link failure - not-operational primitive sequence received.
- Link failure - primitive sequence timeout.
- Link failure - invalid primitive sequence received for current link state.
- **Operational State** - Port state (*Online, Offline, Not Installed, Inactive, Invalid Attachment, Link Reset, No Light, Not Operational, Port Failure, Segmented E_Port, or Testing*). A yellow triangle appears adjacent to the status field if the port is in a non-standard state that requires attention. A red and yellow diamond appears adjacent to the status field if the port fails.
- **Reason** - A summary appears describing the reason if the port state is *Segmented E_Port, Invalid Attachment, or Inactive*. For any other port state, the reason field is blank or N/A.
- **Threshold Alert** - If a threshold alert exists for the port, an alert indicator (yellow triangle) and the configured name for the alert appear.

Port Technology Dialog Box

To open the *Port Technology* dialog box (Figure 4-24), right-click a port graphic at the *Hardware View* or a port row at the *Port List View*, then select *Port Technology* from the pop-up menu.

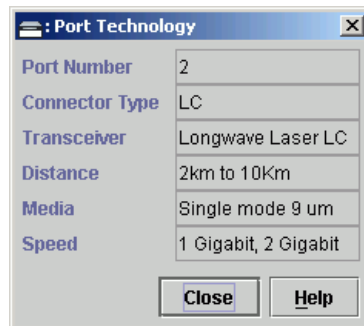


Figure 4-24 Port Technology Dialog Box

The dialog box provides the following information:

- **Port Number** - Switch port number (0 through 23 inclusive).
- **Connector type** - Type of port connector (*LC, Unknown, or Internal Port*).

- **Transceiver** - Type of port transceiver (*Shortwave Laser, Longwave Laser, Long Distance Laser, Unknown, or None*).
- **Distance** - Port transmission distance (*Short, Intermediate, Long, Very Long, or Unknown*).
- **Media** - Type of optical cable used (*Singlemode, multimode 50-micron, multimode 62.5-micron, or Unknown*).
- **Speed** - Operating speed (*Not Established, 1 Gbps, or 2 Gbps*).

Perform Port Diagnostic Loopback Tests

Port diagnostics consist of internal and external loopback tests. The tests are performed on any selected port at the SANpilot interface or the management server (Sphereon 4500 Element Manager application). The tests are described as follows:

- **Internal loopback test** - An internal loopback test checks internal port, serializer, and deserializer circuitry and checks for the presence of an optical transceiver, but does not check fiber-optic components of the installed transceiver. Operation of the attached device is disrupted during the test.
- **External loopback test** - An external loopback test checks all port circuitry, including fiber-optic components of the installed optical transceiver. To perform the test, the attached device must be quiesced and disconnected from the port, and a singlemode or multimode loopback plug must be inserted in the port.

Internal Loopback Test (SANpilot Interface)

To perform an internal loopback at the SANpilot interface:

1. Notify the customer that a disruptive internal loopback test is to be performed. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port, and sets the attached device offline.

NOTE: A small form factor pluggable (SFP) optical transceiver must be installed in the port during the test. A device can remain connected during the test.

2. When the SANpilot interface opens, the *View* panel and *Switch* page appear as the default. At the *View* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens with the *Switch* page displayed.

3. Click the *Port* and *Diagnostics* tabs. The *Port* page displays with the *Diagnostics* tab selected (Figure 4-25).

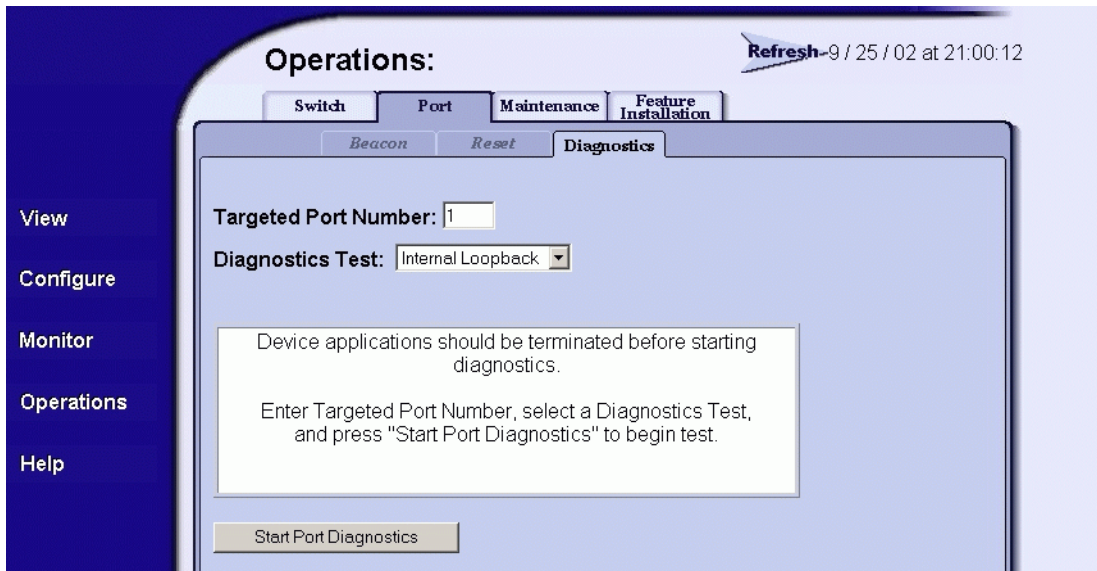


Figure 4-25 Operations Panel (Port Page with Diagnostics Tab)

4. Type the port number to be tested in the *Targeted Port Number* field.
5. At the *Diagnostics Test* list box, select the *Internal Loopback* option.
6. Click *Start Port Diagnostics*. The test begins and:
 - a. The *Start Port Diagnostics* button changes to a *Terminate Port Diagnostics* button.
 - b. The message **Diagnostics Time Remaining: xx** appears, where **xx** are the seconds remaining in the test. The test takes approximately 30 seconds.

NOTE: Click *Terminate Port Diagnostics* at any time to abort the loopback test.

7. When the test completes, results appear as **Passed** or **Failed** in the message area of the dialog box.

8. Reset the tested port:
 - a. Click the *Reset* tab. The *Port* page displays with the *Reset* tab selected.
 - b. For the tested port, click (enable) the check box in the *Port Reset* column. A check mark in the box indicates the port reset option is enabled.
 - c. Click *Activate* at the bottom of the page. The port resets and the message **Your changes have been successfully activated** appears.
9. Notify the customer the test is complete and the attached device can be set online.

External Loopback Test (SANpilot Interface)

To perform an external loopback at the SANpilot interface:

1. Notify the customer that a disruptive external loopback test is to be performed and the attached device must be disconnected.
2. Disconnect the fiber-optic jumper cable from the port to be tested.
3. Depending on the port technology, insert a singlemode or multimode loopback plug into the port receptacle.
4. When the SANpilot interface opens, the *View* panel and *Switch* page appear as the default. At the *View* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens with the *Switch* page displayed.
5. Click the *Port* and *Diagnostics* tabs. The *Port* page displays with the *Diagnostics* tab selected (Figure 4-25 on page 4-39).
6. Type the port number to be tested in the *Targeted Port Number* field.
7. At the *Diagnostics Test* list box, select the *External Loopback* option.
8. Click *Start Port Diagnostics*. The test begins and:
 - a. The *Start Port Diagnostics* button changes to a *Terminate Port Diagnostics* button.
 - b. The message **Diagnostics Time Remaining: xx** appears, where **xx** are the seconds remaining in the test. The test takes approximately 30 seconds.

NOTE: Click *Terminate Port Diagnostics* at any time to abort the loopback test.

9. When the test completes, results appear as **Passed** or **Failed** in the message area of the dialog box.
10. Remove the loopback plug and reconnect the fiber-optic jumper cable from the device to the port (disconnected in [step 2](#)).
11. Reset the tested port:
 - a. Click the *Reset* tab. The *Port* page displays with the *Reset* tab selected.
 - b. For the tested port, click (enable) the check box in the *Port Reset* column. A check mark in the box indicates the port reset option is enabled.
 - c. Click *Activate* at the bottom of the page. The port resets and the message **Your changes have been successfully activated** appears.
12. Notify the customer the test is complete and the device can be reconnected to the switch and set online.

Internal Loopback Test (Management Server)

To perform an internal loopback at the management server (Sphereon 4500 Element Manager application):

1. Notify the customer that a disruptive internal loopback test is to be performed. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port, and sets the attached device offline.

NOTE: A small form factor pluggable (SFP) optical transceiver must be installed in the port during the test. A device can remain connected during the test.

2. At the management server, open the SAN management application (SANavigator 4.0 or EFCM 8.0).
3. At the SAN management application's physical map, right-click the product icon representing the switch to be tested, then select *Element Manager* from the pop-up menu. The application opens.
4. Select the *Port Diagnostics* option from the *Maintenance* menu. The *Port Diagnostics* dialog box displays ([Figure 4-26](#) on page 4-42).

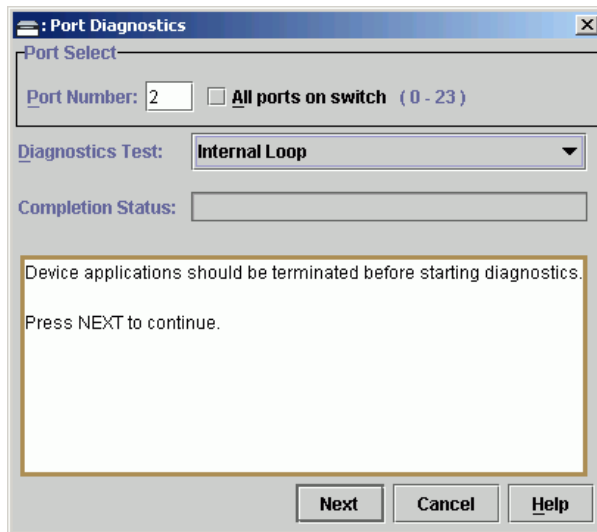


Figure 4-26 Port Diagnostics Dialog Box

5. Type the port number to be tested or select all ports at the *Port Select* area of the dialog box.
 6. At the *Diagnostics Test* list box, select the *Internal Loop* option.
 7. Click *Next*. The message **Press START TEST to begin diagnostics** appears, and the *Next* button changes to a *Start Test* button.
 8. Click *Start Test*. The test begins and:
 - a. The *Start Test* button changes to a *Stop Test* button.
 - b. The message **Port xx: TEST RUNNING** appears.
 - c. A red progress bar (indicating percent completion) travels from left to right across the *Completion Status* field.
- NOTE:** Click *Stop Test* at any time to abort the loopback test.
9. When the test completes, results appear as **Port xx: Passed!** or **Port xx: Failed!** in the message area of the dialog box.
 10. When finished, click *Cancel* to close the *Port Diagnostics* dialog box.

11. Reset the port:
 - a. At the *Hardware View*, right-click the port graphic. A pop-up menu appears.
 - b. Select the *Reset Port* option. A *Message* message box displays, indicating a link reset operation will occur.
 - c. Click OK. The port resets.
12. Notify the customer the test is complete and the attached device can be set online.

External Loopback Test (Management Server)

To perform an external loopback at the management server (Sphereon 4500 Element Manager application):

1. Notify the customer that a disruptive external loopback test is to be performed and the attached device must be disconnected.
2. At the management server, open the SAN management application (SANavigator 4.0 or EFCM 8.0).
3. At the SAN management application's physical map, right-click the product icon representing the switch to be tested, then select *Element Manager* from the pop-up menu. The application opens.
4. Disconnect the fiber-optic jumper cable from the port to be tested.
5. Depending on the port technology, insert a singlemode or multimode loopback plug into the port receptacle.
6. Select the *Port Diagnostics* option from the *Maintenance* menu. The *Port Diagnostics* dialog box displays (Figure 4-26 on page 4-42).
7. Type the port number to be tested or select all ports at the *Port Select* area of the dialog box.
8. At the *Diagnostics Test* list box, select the *External Loop* option.
9. Click *Next*. At the *Port Diagnostics* dialog box, the message **Loopback plug(s) must be installed on ports being diagnosed** appears.
10. Verify a loopback plug is installed and click *Next*. The message **Press START TEST to begin diagnostics** appears, and the *Next* button changes to a *Start Test* button.

11. Click *Start Test*. The test begins and:
 - a. The *Start Test* button changes to a *Stop Test* button.
 - b. The message **Port xx: TEST RUNNING** appears.
 - c. A red progress bar (indicating percent completion) travels from left to right across the *Completion Status* field.

NOTE: Click *Stop Test* at any time to abort the loopback test.

12. When the test completes, results appear as **Port xx: Passed!** or **Port xx: Failed!** in the message area of the dialog box.
13. When finished, click *Cancel* to close the *Port Diagnostics* dialog box.
14. Remove the loopback plug and reconnect the fiber-optic jumper cable from the device to the port (disconnected in [step 4](#)).
15. Reset the port:
 - a. At the *Hardware View*, right-click the port graphic. A pop-up menu appears.
 - b. Select the *Reset Port* option. A *Message* message box displays, indicating a link reset operation will occur.
 - c. Click *OK*. The port resets.
16. Notify the customer the test is complete and the device can be reconnected to the switch and set online.

Collect Maintenance Data

When switch operational firmware detects a critical error, the switch automatically copies the contents of dynamic random access memory (DRAM) to a dump area in FLASH memory on the CTP card, then transfers (through the Ethernet connection) the captured dump file from FLASH memory to the management server hard drive.

NOTE: An optional full-volatility feature is often required at military sites that process classified data. If the feature is enabled through a product feature enablement (PFE) key, a memory dump file (that possibly includes classified Fibre Channel frames) is not included as part of the data collection procedure.

Perform the maintenance data collection procedure after a firmware fault is corrected or a failed FRU is replaced to capture the data for analysis by support personnel. Maintenance data includes the dump file, hardware log, audit log, and an engineering log viewable only by support personnel.

SANpilot Interface

To collect maintenance data (retrieve the dump file from the CTP card) at the SANpilot interface:

1. When the SANpilot interface opens, the *View* panel and *Switch* page appear as the default. At the *View* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens with the *Switch* page displayed.
2. Click the *Maintenance* and *System Files* tabs. The *Maintenance* page displays with the *System Files* tab selected (Figure 4-27).

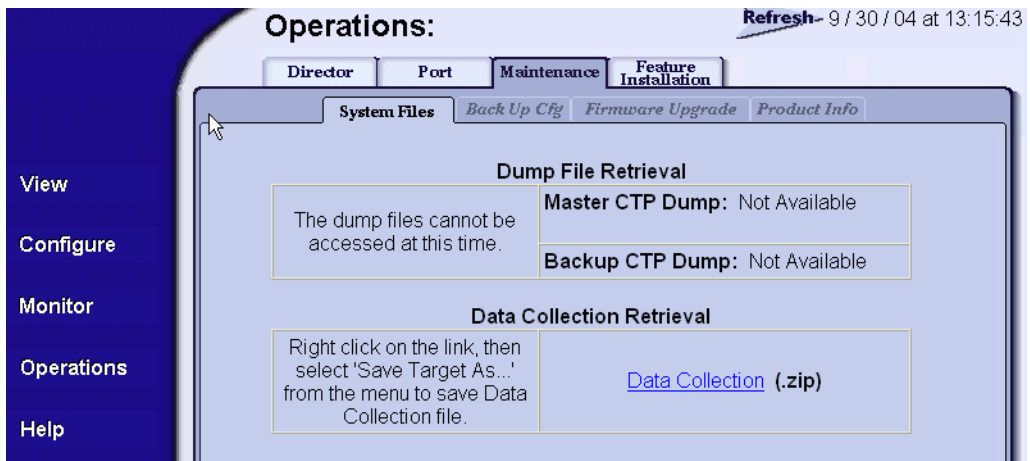


Figure 4-27 Operations Panel (Maintenance Page with System Files Tab)

3. Right-click the *CTP Dump* link to open a list of menu options.
4. Select the *Save Target As* menu option. The *Save As* dialog box displays (Figure 4-28 on page 4-46).

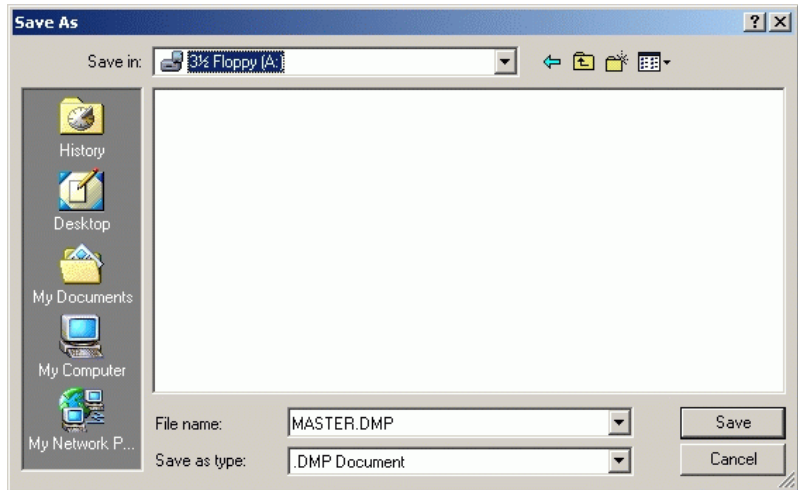


Figure 4-28 Save As Dialog Box

5. Insert a blank diskette in the floppy drive of the browser PC.
6. At the *Save As* dialog box, select the floppy drive (**A:**) from the *Save in* drop-down menu, type a descriptive name for the dump file in the *File name* field, and click *Save*.
7. A *Download* dialog box displays, showing the estimated time remaining to complete the download process. When the process finishes, the dialog box changes to a *Download complete* dialog box ([Figure 4-29](#)).

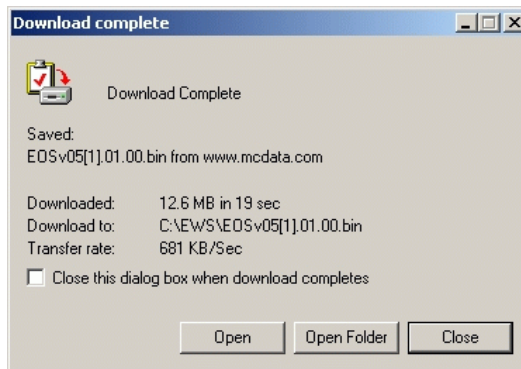


Figure 4-29 Download Complete Dialog Box

Management Server

8. Click *Close* to close the dialog box.
9. Remove the diskette with the newly-collected maintenance data from the browser PC floppy drive. Return the diskette with the failed FRU to McDATA for failure analysis.

To collect maintenance data (retrieve the dump file from the management server hard drive) from the Sphereon 4500 Element Manager application:

1. At the management server, open the SAN management application (SANavigator 4.0 or EFCM 8.0).
2. At the SAN management application's physical map, right-click the product icon representing the switch for which the data collection procedure is to be performed, then select *Element Manager* from the pop-up menu. The application opens.
3. Select the *Data Collection* option from the *Maintenance* menu. The *Save Data Collection* dialog box displays (Figure 4-30).

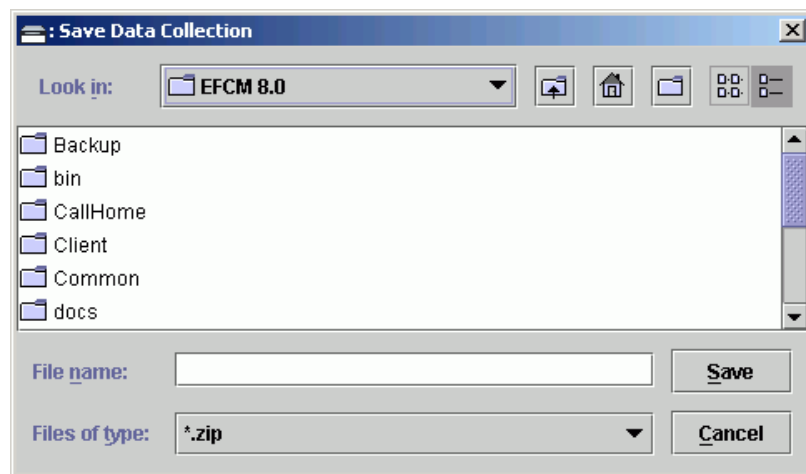


Figure 4-30 Save Data Collection Dialog Box

4. Remove the backup CD from the management server's compact disk-rewritable (CD-RW) drive and insert a blank rewritable CD.

5. At the *Save Data Collection* dialog box, select the compact disc drive (D:\) from the *Look in* drop-down menu, type a descriptive name for the collected maintenance data in the *File name* field, then click *Save*.
6. The *Data Collection* dialog box (Figure 4-31) displays with a progress bar that shows percent completion of the data collection process. When the process reaches 100%, the *Cancel* button changes to a *Close* Button.

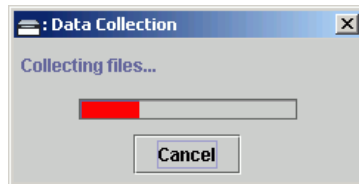


Figure 4-31 Data Collection Dialog Box

7. Click *Close* to close the dialog box.
8. Remove the CD with the newly-collected maintenance data from the management server's CD-RW drive. Return the CD with the failed FRU to McDATA for failure analysis.
9. To ensure the backup application operates normally, replace the original backup CD in the management server's CD-RW drive.

Set the Switch Online or Offline

This section describes procedures to set the switch online or offline. These operating states are described as follows:

- **Online** - When the switch is set online, an attached device can log in to the switch if the port is not blocked. Attached devices can communicate with each other if they are configured in the same zone.
- **Offline** - When the switch is set offline, all switch ports are set offline. The switch transmits the offline sequence (OLS) to attached devices, and the devices cannot log in to the switch.

NOTE: When the switch is set offline, the operation of attached Fibre Channel devices is disrupted. Do not set the switch offline unless directed to do so by a procedural step or the next level of support.

Set Online State (SANpilot Interface)

To set the switch online from the SANpilot interface:

1. When the SANpilot interface opens, the *View* panel and *Switch* page appear as the default. At the *View* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens with the *Switch* page displayed.
2. Click the *Online State* tab. The *Switch* page displays with the *Online State* tab selected (Figure 4-32).

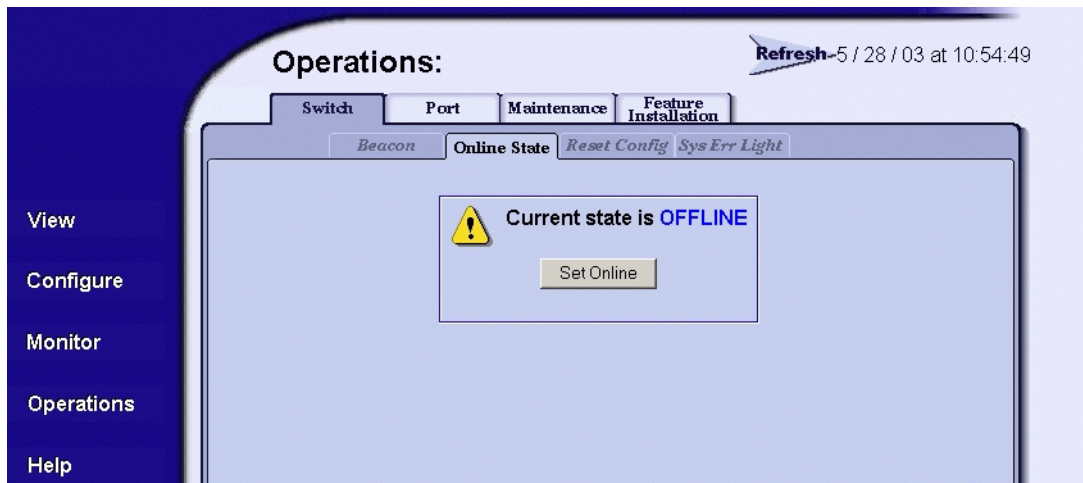


Figure 4-32 Operations Panel (Switch Page with Online State Tab)

3. Click Set Online. The switch comes online and the message **Your changes have been successfully activated** appears.

Set Offline State (SANpilot Interface)

To set the switch offline from the SANpilot interface:

1. When the SANpilot interface opens, the *View* panel and *Switch* page appear as the default. At the *View* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens with the *Switch* page displayed.

Set Online State (Management Server)

2. Click the *Online State* tab. The *Switch* page displays with the *Online State* tab selected (Figure 4-32 on page 4-49).
3. Click Set Offline. The switch goes offline and the message **Your changes have been successfully activated** appears.

To set the switch online from the management server (Sphereon 4500 Element Manager application):

1. At the management server, open the SAN management application (SANavigator 4.0 or EFCM 8.0).
2. At the SAN management application's physical map, right-click the product icon representing the switch to be set online, then select *Element Manager* from the pop-up menu. The application opens.
3. Select the *Set Online State* option from the *Maintenance* menu. The *Set Online State* dialog box displays (Figure 4-33).



Figure 4-33 Set Online State Dialog Box

4. Click *Set Online*. A warning dialog box displays the message **Performing this operation will change the current state to Online**.
5. Click OK. As the switch comes online, inspect the *Hardware View*. The *State* field of the *Sphereon 4500 Status* table displays **Online**.

Set Offline State (Management Server)

To set the switch offline from the management server (Sphereon 4500 Element Manager application):

1. At the management server, open the SAN management application (SANavigator 4.0 or EFCM 8.0).
2. At the SAN management application's physical map, right-click the product icon representing the switch to be set offline, then select *Element Manager* from the pop-up menu. The application opens.

3. Select the *Set Online State* option from the *Maintenance* menu. The *Set Online State* dialog box displays (Figure 4-33 on page 4-50).
4. Click *Set Offline*. A warning dialog box displays the message **Performing this operation will change the current state to Offline.**
5. Click *OK*. As the switch goes offline, inspect the *Hardware View*. The *State* field of the *Sphereon 4500 Status* table displays **Offline**.

Block or Unblock a Port

This section describes procedures to block or unblock a switch Fibre Channel port. Blocking a port prevents the attached device or fabric switch from communicating. A blocked port continuously transmits the offline sequence (OLS).

Block a Port (SANpilot Interface)

To block a switch port from the SANpilot interface:

1. When the SANpilot interface opens, the *View* panel and *Switch* page appear as the default. At the *View* panel, select the *Configure* option at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed (Figure 4-34).

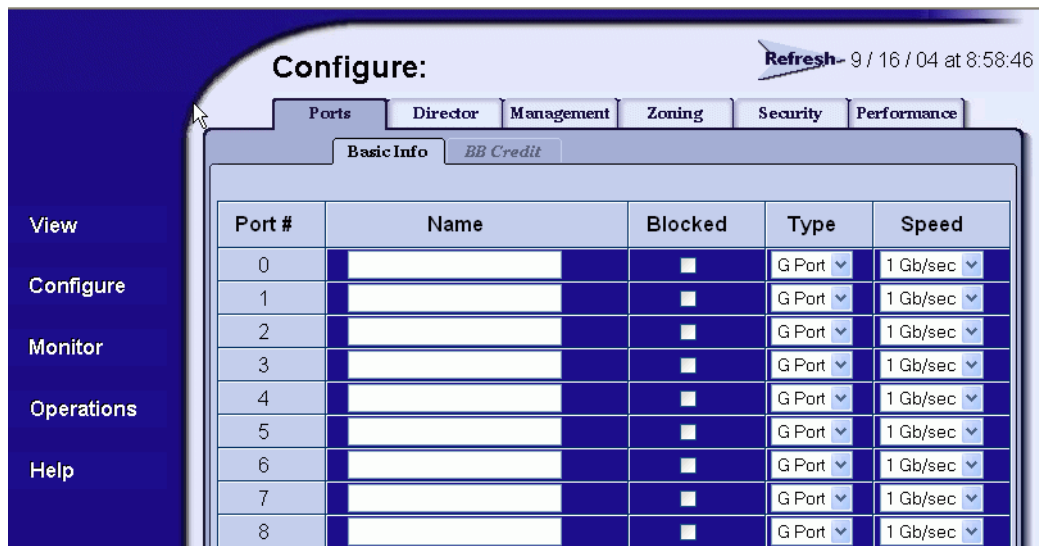


Figure 4-34 Configure Panel (Ports Page)

2. Click the check box for the selected port in the *Blocked* column to block the port (default is unblocked). A check mark in the box indicates the port is blocked.
3. Click *Activate* at the bottom of the page to save and activate the blocked configuration. The message **Your changes to the port configuration have been successfully activated** appears.

Unblock a Port (SANpilot Interface)

To unblock a switch port from the SANpilot interface:

1. When the SANpilot interface opens, the *View* panel and *Switch* page appear as the default. At the *View* panel, select the *Configure* option at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed (Figure 4-34 on page 4-51).
2. Click the check box for the selected port in the *Blocked* column to remove the check mark and unblock the port. A blank box indicates the port is unblocked.
3. Click *Activate* at the bottom of the page to save and activate the unblocked configuration. The message **Your changes to the port configuration have been successfully activated** appears.

Block a Port (Management Server)

To block a switch port from the management server (Sphereon 4500 Element Manager application):

1. Notify the customer that a port is to be blocked. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port.
2. At the management server, open the SAN management application (SANavigator 4.0 or EFCM 8.0).
3. At the SAN management application's physical map, right-click the product icon representing the switch for which the port is to be blocked, then select *Element Manager* from the pop-up menu. The application opens.
4. Click the *Hardware* tab. The *Hardware View* for the selected switch displays.
5. Move the cursor over the port to be blocked and right-click the mouse to open a list of menu options.

6. Select the *Block Port* menu option. A *Warning* dialog box displays (Figure 4-35).

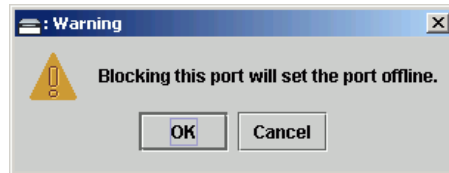


Figure 4-35 Warning Dialog Box

7. Click *OK*. The dialog box closes and the following occur to indicate the port is blocked and offline:
 - The emulated green LED associated with the port extinguishes at the *Hardware View*.
 - The green LED associated with the port extinguishes at the switch.
 - A check mark displays in the check box adjacent to the *Block Port* menu option.

Unblock a Port (Management Server)

To unblock a switch port from the management server (Sphereon 4500 Element Manager application):

1. At the management server, open the SAN management application (SANavigator 4.0 or EFCM 8.0).
2. At the SAN management application's physical map, right-click the product icon representing the switch for which the port is to be unblocked, then select *Element Manager* from the pop-up menu. The application opens.
3. Click the *Hardware* tab. The *Hardware View* for the selected switch displays.
4. Move the cursor over the port to be unblocked and right-click the mouse to open a list of menu options.
5. Select the *Block Port* menu option. Note the check mark in the box adjacent to the menu item, indicating the port is blocked. A *Warning* dialog box displays (Figure 4-36 on page 4-54).

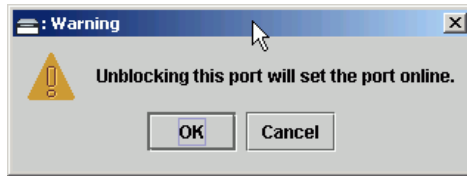


Figure 4-36 Warning Dialog Box

6. Click OK. The dialog box closes and the following occur to indicate the port is unlocked (and online):
 - The emulated green LED associated with the port illuminates at the *Hardware View*.
 - The green LED associated with the port illuminates at the switch.
 - The check box adjacent to the *Block Port* menu option becomes blank.

Clean Fiber-Optic Components

Perform this procedure as directed in this publication and when connecting or disconnecting fiber-optic cables from port optical transceivers (if necessary). To clean fiber-optic components:

1. Obtain the appropriate tools (portable can of oil-free compressed air and alcohol pads) from the fiber-optic cleaning kit.
2. Disconnect the fiber-optic cable from the transceiver. Use compressed air to blow any contaminants from the connector as shown in part **A** of [Figure 4-37](#).

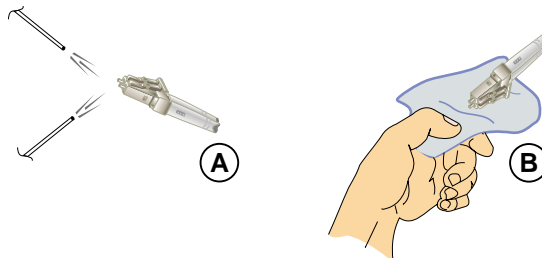


Figure 4-37 Clean Fiber-Optic Components

- Keep the air nozzle approximately 50 millimeters (two inches) from the end of the connector and hold the can upright.
 - Blow compressed air on the surfaces and end of the connector continuously for approximately five seconds.
3. Gently wipe the end-face and other surfaces of the connector with an alcohol pad as shown in part **B** of [Figure 4-37](#) on page 4-54. Ensure the pad makes full contact with the surface to be cleaned. Wait approximately five seconds for cleaned surfaces to dry.
 4. Repeat [step 2](#) and [step 3](#) of this procedure (second cleaning).
 5. Repeat [step 2](#) and [step 3](#) of this procedure again (third cleaning), then reconnect the fiber-optic cable to the port.

Power-On Procedure

To power on the switch:

1. One alternating current (AC) power cord is required for each power supply. Ensure power cord(s) are available to connect the switch to facility power.



DANGER

Use the supplied power cords. Ensure the facility power receptacle is the correct type, supplies the required voltage, and is properly grounded.

2. Plug the power cord(s) into facility power sources and power supply AC connectors at the rear of the switch. When the first power cord is connected, the switch powers on and performs power-on self-tests (POSTs).

NOTE: If two power cords are used for high availability, plug the cords into separate facility power circuits.

3. During POSTs:
 - The green power (**PWR**) LED on the switch front panel illuminates.
 - The amber system error (**ERR**) LED on the switch front panel blinks momentarily while the switch is tested.

- The green LED associated with the Ethernet port blinks momentarily while the port is tested.
 - The blue/green and amber LEDs associated with the ports blink momentarily while the ports are tested.
4. After successful POST completion, the green power (**PWR**) LED remains illuminated and all amber LEDs extinguish.
 5. If a POST error or other malfunction occurs, go to [MAP 0000: Start MAP](#) on page 3-6 to isolate the problem.

Power-Off Procedure

To power off the switch:

1. Notify the customer the switch is to be powered off. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the switch and sets attached FC-AL devices offline.
2. Set the switch offline. For instructions, refer to [Set the Switch Online or Offline](#) on page 4-48.
3. Disconnect power cord(s) from the power supply AC connectors at the rear of the switch.

IML, IPL, or Reset the Switch

This section describes procedures to IML, IPL, or reset the Sphereon 4500 Switch. An IML or reset is performed at the switch front panel using the **IML/RESET** button. An IPL is performed from the management server (Element Manager application). The SANpilot interface does not provide an IML, IPL, or switch reset function.

ATTENTION ! A reset should only be performed if a CTP card failure is indicated. Do not reset a managed product unless directed to do so by a procedural step or the next level of support.

An IML and IPL are functionally equivalent. The operations do not cause power-on diagnostics to execute and are not disruptive to Fibre Channel traffic. Both operations:

- Reload switch firmware from FLASH memory.
- Reset the Ethernet LAN interface, causing the connection to the management server to drop momentarily until the connection automatically recovers.

A switch reset is more disruptive and resets the:

- Microprocessor and functional logic for the CTP card and reloads the firmware from FLASH memory.
- Ethernet LAN interface, causing the connection to the management server to drop momentarily until the connection automatically recovers.
- Ports, causing all Fibre Channel connections to drop momentarily until the connections automatically recover. This causes attached devices to log out and log back in, therefore data frames lost during switch reset must be retransmitted.

Switch IML

To IML the switch from the front panel:

1. Press and hold the **IML/RESET** button until the amber **ERR** LED blinks at twice the unit beaoning rate (approximately three seconds).
2. Release the button to IML the switch. During the IML, the switch-to-management server Ethernet link drops momentarily and the following occur at the *Hardware View*:
 - As the network connection drops, the *Sphereon 4500 Status* table turns yellow, the *Status* field displays **No Link**, and the *State* field displays **Link Timeout**.
 - The status bar at the bottom of the window displays a grey square, indicating switch status is unknown.
 - Illustrated FRUs disappear, and appear again as the connection is re-established.

Switch IPL

To IPL the switch from the management server (Sphereon 4500 Element Manager application):

1. At the management server, open the SAN management application (SANavigator 4.0 or EFCM 8.0).
2. At the SAN management application's physical map, right-click the product icon representing the switch requiring an IPL, then select *Element Manager* from the pop-up menu. The application opens.
3. Select the *IPL* option from the *Maintenance* menu. An *Information* dialog box displays (Figure 4-38).

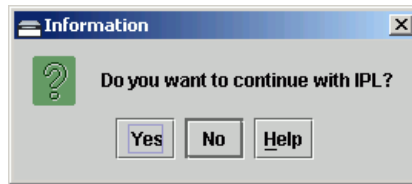


Figure 4-38 Information Dialog Box

4. Click *Yes* to IPL the switch. During the IPL, the switch-to-management server Ethernet link drops momentarily and the following occur at the *Hardware View*:
 - As the network connection drops, the *Sphereon 4500 Status* table turns yellow, the *Status* field displays **No Link**, and the *State* field displays **Link Timeout**.
 - The status bar at the bottom of the window displays a grey square, indicating switch status is unknown.
 - Illustrated FRUs disappear, and appear again as the connection is re-established.

Switch Reset

To reset the switch from the front panel:

1. Press and hold the **IML/RESET** button for approximately ten seconds.
 - After holding the button for three seconds, the amber **ERR** LED blinks at twice the unit beaoning rate.

- After holding the button for ten seconds, the **ERR** LED stops blinking, and all front panel LEDs illuminate.
- 2. Release the button to reset the switch. During the reset:
 - The green power (**PWR**) LED on the switch front panel illuminates.
 - The amber system error (**ERR**) LED on the switch front panel blinks momentarily while the switch is tested.
 - The green LED associated with the Ethernet port blinks momentarily while the port is tested.
 - The blue/green and amber LEDs associated with the ports blink momentarily while the ports are tested.
 - The switch-to-management server Ethernet link drops momentarily and the following occur at the *Hardware View*:
 - As the network connection drops, the *Sphereon 4500 Status* table turns yellow, the *Status* field displays **No Link**, and the *State* field displays **Link Timeout**.
 - The status bar at the bottom of the window displays a grey square, indicating switch status is unknown.
 - Illustrated FRUs disappear, and appear again as the connection is re-established.

Manage Firmware Versions

Firmware is the switch operating code stored in FLASH memory on the CTP card. Multiple firmware versions can be stored on a browser PC hard drive and made available for download to the switch from the SANpilot interface. Up to 32 firmware versions can be stored on the management server hard drive and made available for download to a switch through the Sphereon 4500 Element Manager application.

SANpilot Interface

Service personnel can perform the following firmware management tasks from the SANpilot interface:

- Determine the firmware version actively running on the switch.
- Add a firmware versions to the browser PC hard drive.
- Download a firmware version to the switch.

Determine Switch Firmware Version

To determine a switch firmware version from the SANpilot interface:

1. When the SANpilot interface opens, the *View* panel and *Switch* page appear as the default. At the *View* panel, click the *Unit Properties* tab. The *Unit Properties* page displays (Figure 4-39).

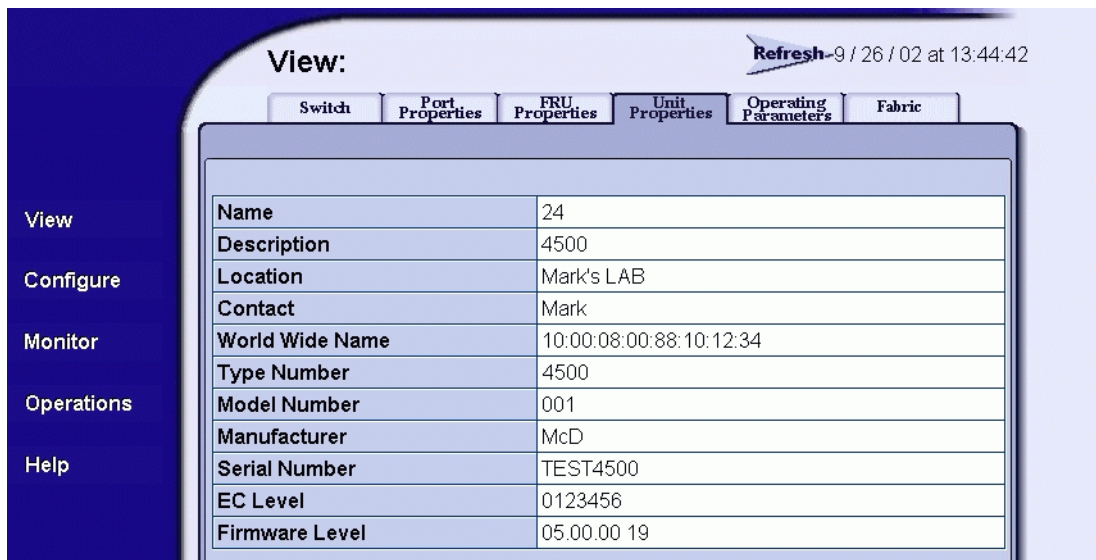


Figure 4-39 View Panel (Unit Properties Page)

2. At the bottom of the page, record the firmware version listed in the *Firmware Level* field.

Add a Firmware Version to the Browser PC Hard Drive

The firmware version shipped with the switch is provided on the *System Version XX.YY.ZZ* CD-ROM. Subsequent firmware versions for upgrading the switch are provided to customers through McDATA's Internet home page.

NOTE: When adding a firmware version, follow all procedural information contained in release notes or engineering change (EC) instructions that accompany the code. This information supplements information provided in this general procedure.

To add a switch firmware version to the browser PC hard drive (PC running the SANpilot interface):

1. Obtain the new firmware version from the McDATA File Center. At a PC with Internet access, open the File Center home page ([Figure 4-40](#)). The uniform resource locator (URL) is <http://central.mcddata.com>.

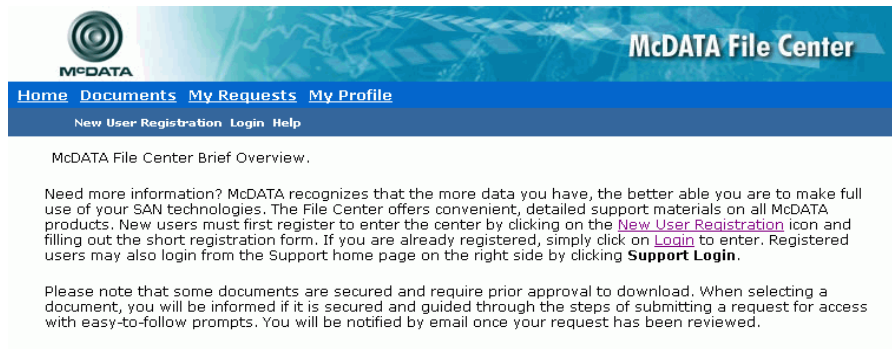


Figure 4-40 McDATA File Center Home Page

2. Select (click) the *Login* option at the top of the home page. The *Login* page displays ([Figure 4-41](#)).

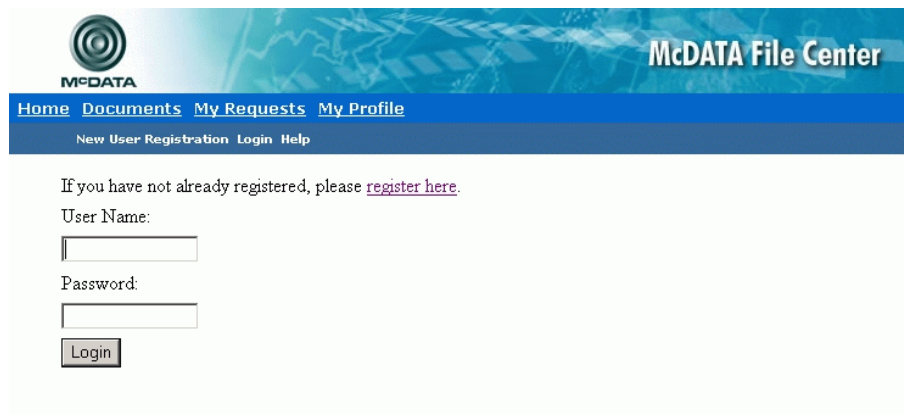


Figure 4-41 McDATA File Center (Login Page)


3. Type the user name and password (assigned and registered while performing [Task 24: Register with the McDATA File Center](#) on page 2-127) and click *Login*. The *Welcome* page displays.
4. Select (click) the *Documents* option at the top of the page. The *Find Documents* page displays ([Figure 4-42](#)).

Find documents where

<input checked="" type="checkbox"/>	Category is one or more of the following	Select..... ES 4500 Documentation ES 4500 Firmware ED 6064 Documentation
<input type="checkbox"/>	And the title contains one or more of the following words	<input type="text"/>
<input type="checkbox"/>	And the description contains one or more of the following words	<input type="text"/>

Figure 4-42 McDATA File Center (Find Documents Page)

5. Select (highlight) the *ES 4500 Firmware* option at the list box and click *Search*. The *Documents Match* page displays ([Figure 4-43](#) on page 4-63) with a list of firmware available for download.



McDATA File Center

Home Documents My Requests My Profile

Search New Documents By Category

The following documents match your search criteria.

Showing 1-3 of 3 items.



Status	Action	Size	Title	Description	Online Date	Offline Date
	Add To Request	13260k	EOS 5.01	EOS 5.01 has been approved for McDATA only at this point. It is not yet approved for installation on EMC, IBM, HPQ, STK or HDS accounts. McDATA E/OS firmware version 05.01.00 is supported on the following products: Intrepid™ 6140 (ED-6140) Intrepid 6064 (ED-6064) Sphereon™ 3016 (Model 001 and 002) Sphereon 3032 (Model 001 and 002) Sphereon 3216 Sphereon 3232 Sphereon 4500	05/01/2003	

Figure 4-43 McDATA File Center (Documents Match Page)

6. Authorization to download a firmware version requires approval from the McDATA Solution Center. In the *Action* column adjacent to the desired firmware version, click *Add to Request*. The *Current Request* page displays (Figure 4-44).



McDATA File Center

Home Documents My Requests My Profile

History Current

Current Request: Not Yet Submitted

Action	Title	Description
Remove	EOS 5.01	EOS 5.01 has been approved for McDATA only at this point. It is not yet approved for installation on EMC, IBM, HPQ, STK or HDS accounts. McDATA E/OS firmware version 05.01.00 is supported on the following products: Intrepid™ 6140 (ED-6140) Intrepid 6064 (ED-6064) Sphereon™ 3016 (Model 001 and 002) Sphereon 3032 (Model 001 and 002) Sphereon 3216 Sphereon 3232 Sphereon 4500

[Submit Request](#)

Figure 4-44 McDATA File Center (Current Request Page)

7. Click *Submit Request*. The *Request Submitted* page displays and the request for approval is e-mailed to the McDATA Solution Center. Wait five to ten minutes for a response from McDATA, then select (click) the *My Requests* option at the top of the page. The *Request History* page displays (Figure 4-45 on page 4-64) with the approved request.

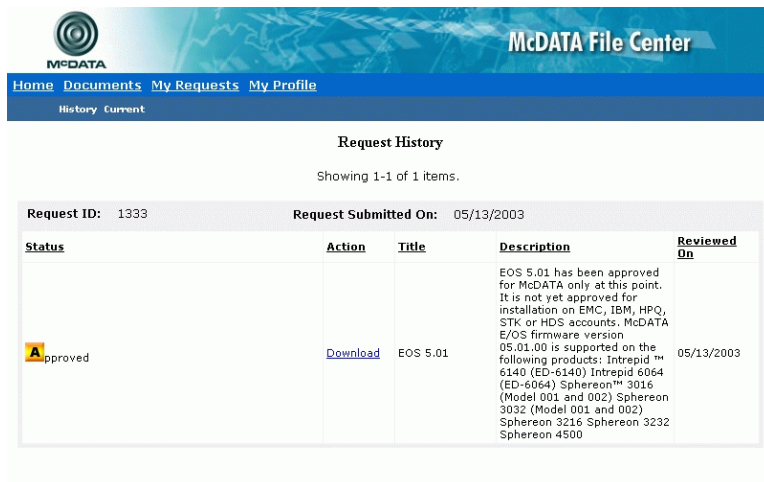


Figure 4-45 McDATA File Center (Request History Page)

8. In the *Action* column adjacent to the approved request for the firmware version, click *Download*. The *File Download* dialog box displays (Figure 4-46).

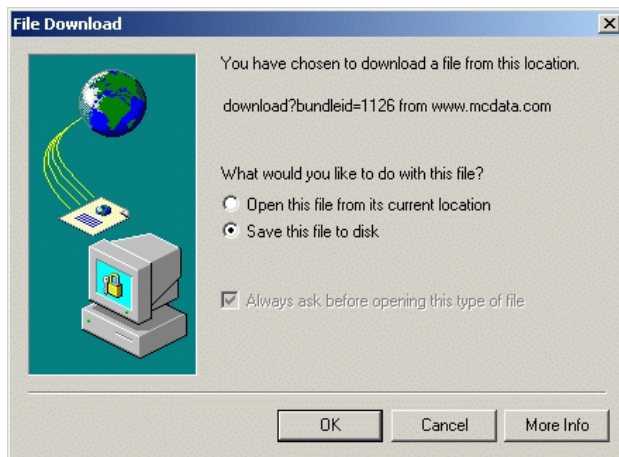


Figure 4-46 File Download Dialog Box

9. Select the *Save this file to disk* radio button and click *OK*. The *Save As* dialog box appears (Figure 4-47 on page 4-65).

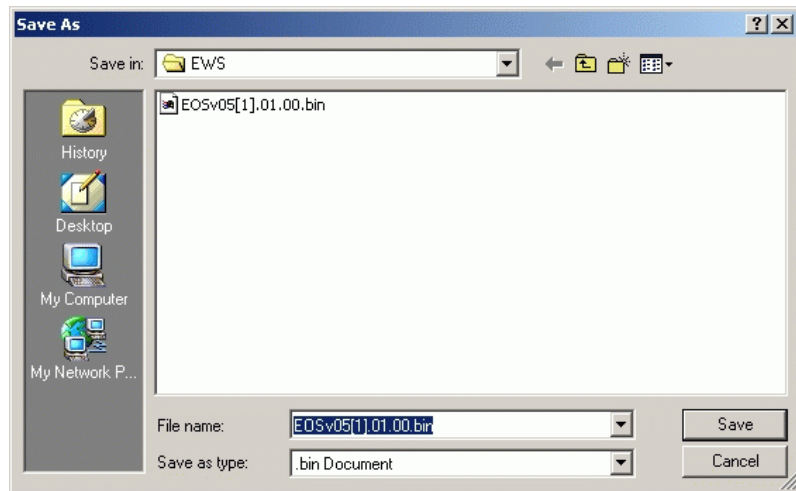


Figure 4-47 Save As Dialog Box

10. At the *Save As* dialog box, ensure the correct directory path is specified at the *Save in* field, the correct file is specified in the *File name* field, and click *Save*.
11. A *Download* dialog box displays, showing the estimated time remaining to complete the download process. When the process finishes, the dialog box changes to a *Download complete* dialog box (Figure 4-48).

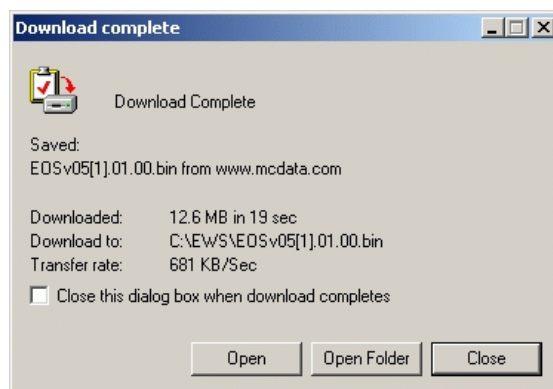


Figure 4-48 Download Complete Dialog Box

12. Click *Close* to close the dialog box. The new firmware version is downloaded and saved to the browser PC hard drive.
13. At the browser PC, close the Internet session.

Download a Firmware Version to the Switch

To download a firmware version to the switch from the SANpilot interface:

NOTE: When downloading a firmware version, follow all procedural information contained in release notes or EC instructions that accompany the firmware version. This information supplements information provided in this general procedure.

1. When the SANpilot interface opens, the *View* panel and *Switch* page appear as the default. At the *View* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens with the *Switch* page displayed.
2. Click the *Maintenance* and *Firmware Upgrade* tabs. The *Maintenance* page displays with the *Firmware Upgrade* tab selected (Figure 4-49).

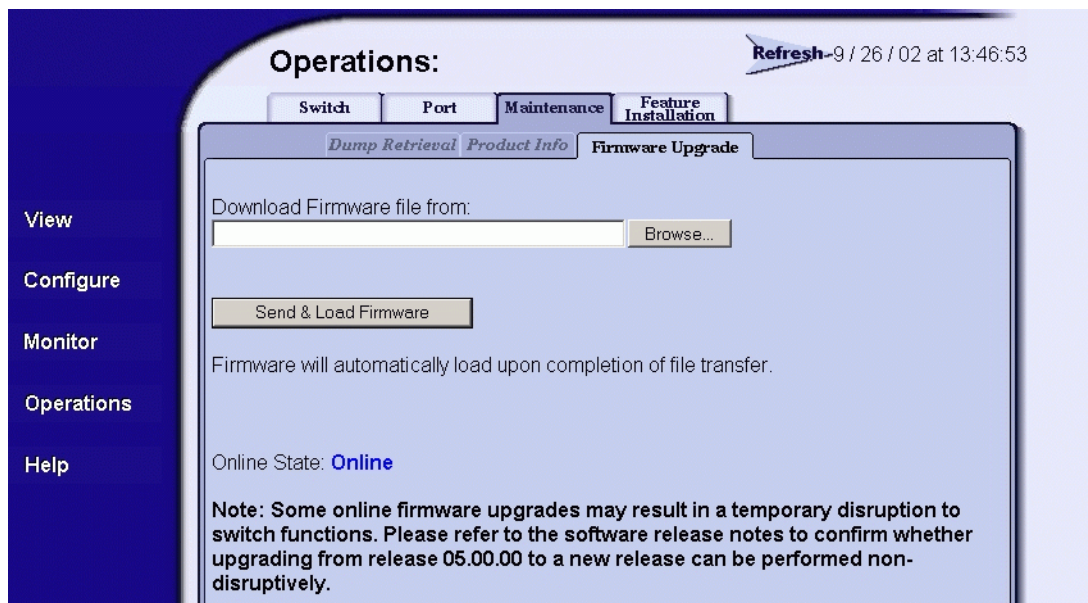


Figure 4-49 Operations Panel (Maintenance Page with Firmware Upgrade Tab)

3. At the *Download Firmware file from* field:
 - Select the desired firmware file from the PC hard drive using the *Browse* button, or
 - Type the desired firmware filename in the *Download Firmware file from* field.
4. Click *Send and Load Firmware*. A browser-specific message box displays (Figure 4-50).

```

Security Log
Reason  Date/Time          Trigger Level      Count
-----
10000  09/30/2004 11:47:12    Informational      1
Category: Successful Connection
Description: EMS User Connected
Data:      User name = 'Administrator' IP address = 127.000.000.001 Role =
          administrator Protocol = http
10400  09/30/2004 11:47:05     Error              1
Category: Authentication Failure
Description: EMS Wrong User Name - Password Combination
Data:      User name = Administrator IP address = 127.000.000.001
10000  09/30/2004 11:46:59    Informational      1
Category: Successful Connection
Description: EMS User Connected
Data:      User name = 'Administrator' IP address = 127.000.000.001 Role =
          administrator Protocol = http

```

Figure 4-50 Browser-Specific Message Box

5. Click *OK* to download the firmware version to the switch. The download process takes several minutes to complete, during which the browser is unavailable.
6. When the firmware version is downloaded to the switch and verified, the following message box displays (Figure 4-51).

**Firmware successfully received and verified.
Your browser connection will be unavailable
until unit restart is complete.**

If your browser is not redirected to the Firmware
Complete Acknowledgement page within 30
seconds, click [here](#).

Figure 4-51 Firmware Received Message Box

7. After firmware verification, the switch performs an IPL that takes approximately 30 seconds to complete. During the IPL, the browser-to-switch Internet connection drops momentarily and the SANpilot session is lost.

8. After the switch IPL and SANpilot session logout, the following message box displays (Figure 4-52).



Figure 4-52 Firmware Upgrade Complete Message Box

9. Click [here](#) to login to the switch and start a new SANpilot session. The *Enter Network Password* dialog box displays.
10. Type the default user name and password.

NOTE: The default user name is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

11. Click OK. The SANpilot interface opens with the *View* panel open and the *Switch* page displayed.

Management Server

Service personnel can perform the following firmware management tasks from the management server (Sphereon 4500 Element Manager application):

- Determine the firmware version actively running on a selected switch.
- Add to and maintain a library of up to 32 firmware versions on the management server hard drive.
- Download a firmware version to a selected switch.

Determine Switch Firmware Version

To determine a switch firmware version from the management server (Sphereon 4500 Element Manager application):

1. At the management server, open the SAN management application (SANavigator 4.0 or EFCM 8.0).
2. At the SAN management application's physical map, right-click the product icon representing the switch to be inspected for firmware version, then select *Element Manager* from the pop-up menu. The application opens.

3. Select the *Firmware Library* option from the *Maintenance* menu. The *Firmware Library* dialog box displays (Figure 4-53).

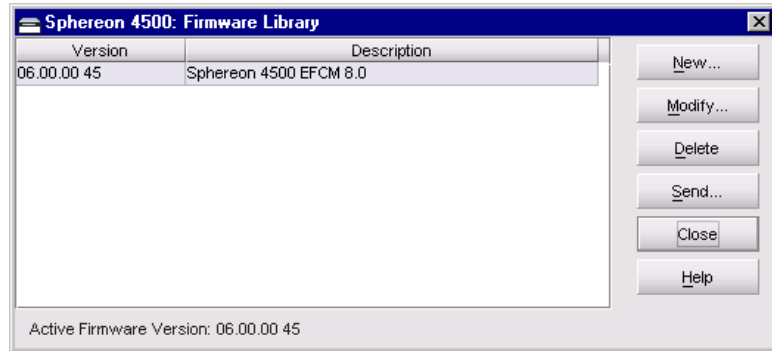


Figure 4-53 Firmware Library Dialog Box

4. The active firmware version displays at the lower left corner of the dialog box in *XX.YY.ZZ* format, where *XX* is the version level, *YY* is the release level, and *ZZ* is the patch level.
5. Click *Close* to close the dialog box.

Add a Firmware Version to the Management Server Library

The firmware version shipped with the switch is provided on the *System Version XX.YY.ZZ* CD-ROM. Subsequent firmware versions for upgrading the switch are provided to customers through McDATA's Internet home page.

NOTE: When adding a firmware version, follow all procedural information contained in release notes or engineering change (EC) instructions that accompany the code. This information supplements information provided in this general procedure.

To add a switch firmware version to the library stored on the management server hard drive:

1. Obtain the new firmware version from the McDATA File Center:
 - a. At a PC with Internet access, open the File Center home page (Figure 4-54 on page 4-70). The URL is <http://central.mcdata.com>.

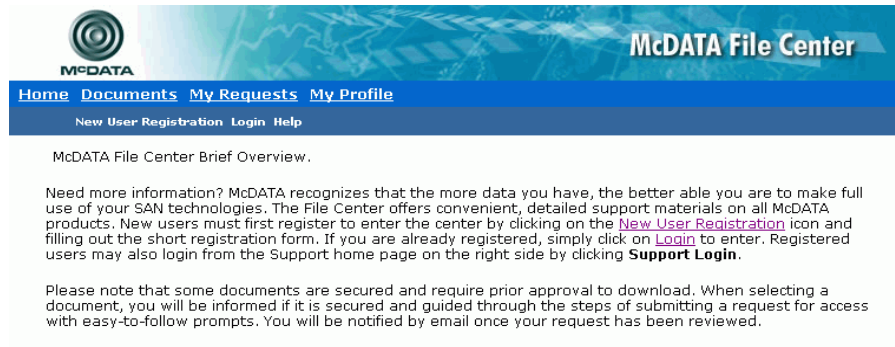


Figure 4-54 McDATA File Center Home Page

- b. Select (click) the *Login* option at the top of the home page. The *Login* page displays (Figure 4-41 on page 4-61).
- c. Type the user name and password (assigned and registered while performing *Task 24: Register with the McDATA File Center* on page 2-127) and click *Login*. The *Welcome* page displays.
- d. Select (click) the *Documents* option at the top of the page. The *Find Documents* page displays (Figure 4-55).

McDATA File Center

[Home](#) [Documents](#) [My Requests](#) [My Profile](#)

[Search](#) [New Documents](#) [By Category](#)

Click the check boxes on the left of each search option to include it in the search criteria. Then fill in any requested data for that search criteria. This helps narrow the search to give you more accurate search results.

Find documents where

<input checked="" type="checkbox"/>	Category is one or more of the following	Select..... ES 4500 Documentation ES 4500 Firmware ED 6064 Documentation
<input type="checkbox"/>	And the title contains one or more of the following words	<input type="text"/>
<input type="checkbox"/>	And the description contains one or more of the following words	<input type="text"/>

Figure 4-55 McDATA File Center (Find Documents Page)

- e. Select (highlight) the *ES 4500 Firmware* option at the list box and click *Search*. The *Documents Match* page displays (Figure 4-56) with a list of firmware available for download.

The screenshot shows the McDATA File Center interface. At the top, there is a navigation bar with links: Home, Documents, My Requests, and My Profile. Below this is a search bar with the text "Search New Documents By Category". The main content area displays the message "The following documents match your search criteria." followed by "Showing 1-3 of 3 items." Below this is a table with the following data:

Status	Action	Size	Title	Description	Online Date	Offline Date
	Add To Request	13260k	EOS 5.01	EOS 5.01 has been approved for McDATA only at this point. It is not yet approved for installation on EMC, IBM, HPQ, STK or HDS accounts. McDATA E/OS firmware version 05.01.00 is supported on the following products: Intrepid™ 6140 (ED-6140) Intrepid 6064 (ED-6064) Sphereon™ 3016 (Model 001 and 002) Sphereon 3032 (Model 001 and 002) Sphereon 3216 Sphereon 3232 Sphereon 4500	05/01/2003	

Figure 4-56 McDATA File Center (Documents Match Page)

- f. Authorization to download a firmware version requires approval from the McDATA Solution Center. In the *Action* column adjacent to the desired firmware version, click *Add to Request*. The *Current Request* page displays (Figure 4-57).

The screenshot shows the McDATA File Center interface. At the top, there is a navigation bar with links: Home, Documents, My Requests, and My Profile. Below this is a search bar with the text "Search New Documents By Category". The main content area displays the message "Current Request: Not Yet Submitted" followed by a table with the following data:

Action	Title	Description
Remove	EOS 5.01	EOS 5.01 has been approved for McDATA only at this point. It is not yet approved for installation on EMC, IBM, HPQ, STK or HDS accounts. McDATA E/OS firmware version 05.01.00 is supported on the following products: Intrepid™ 6140 (ED-6140) Intrepid 6064 (ED-6064) Sphereon™ 3016 (Model 001 and 002) Sphereon 3032 (Model 001 and 002) Sphereon 3216 Sphereon 3232 Sphereon 4500

Below the table is a button labeled "Submit Request".

Figure 4-57 McDATA File Center (Current Request Page)

- g. Click *Submit Request*. The *Request Submitted* page displays and the request for approval is e-mailed to the McDATA Solution Center. Wait five to ten minutes for a response from McDATA, then select (click) the *My Requests* option at the top of the page. The *Request History* page displays (Figure 4-58) with the approved request.



Figure 4-58 McDATA File Center (Request History Page)

- h. In the *Action* column adjacent to the approved request for the firmware version, click *Download*. The *File Download* dialog box displays (Figure 4-59).

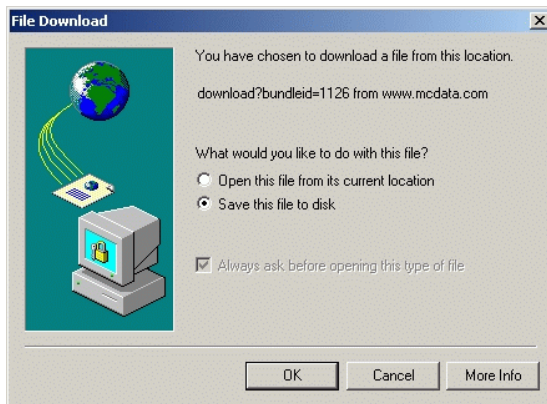


Figure 4-59 File Download Dialog Box

- i. Select the *Save this file to disk* radio button and click *OK*. The *Save As* dialog box appears (Figure 4-60).

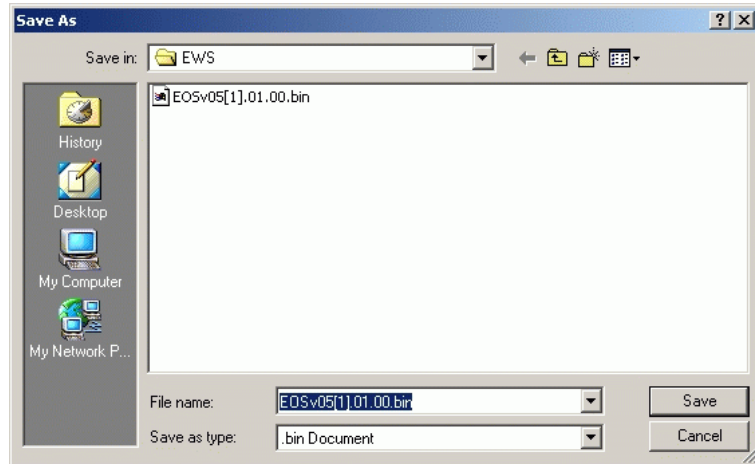


Figure 4-60 Save As Dialog Box

- j. At the *Save As* dialog box, ensure the correct directory path is specified at the *Save in* field, the correct file is specified in the *File name* field, and click *Save*.
- k. A *Download* dialog box displays, showing the estimated time remaining to complete the download process. When the process finishes, the dialog box changes to a *Download complete* dialog box (Figure 4-61).

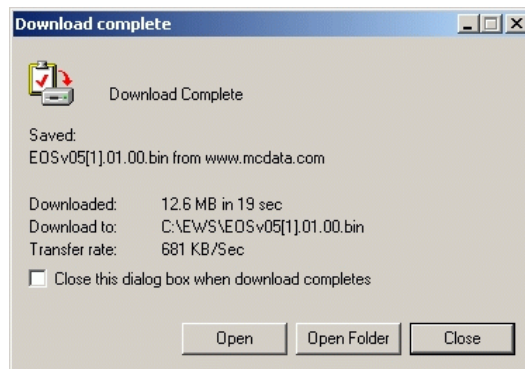


Figure 4-61 Download Complete Dialog Box

1. Click *Close* to close the dialog box. The new firmware version is downloaded and saved to the PC hard drive.
- m. At the PC, close the Internet session.
- n. Transfer the firmware version file from the PC to the rack-mount management server by diskette, CD-ROM, or other electronic means.
2. At the management server, open the SAN management application (SANavigator 4.0 or EFCM 8.0).
3. At the SAN management application's physical map, right-click the product icon representing the switch for which a firmware version is to be added, then select *Element Manager* from the pop-up menu. The application opens.
4. Select the *Firmware Library* option from the *Maintenance* menu. The *Firmware Library* dialog box displays (Figure 4-62).

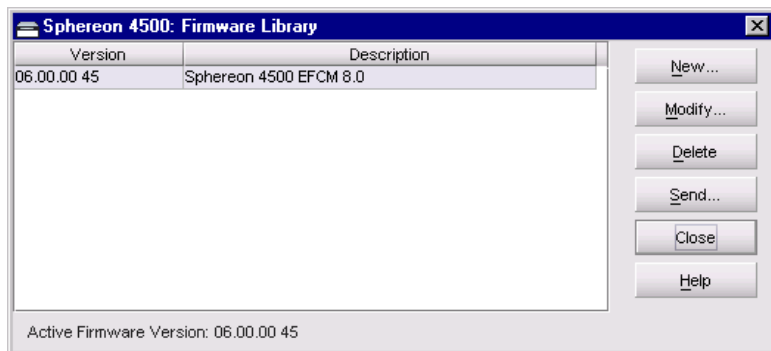


Figure 4-62 Firmware Library Dialog Box

5. Click *New*. The *New Firmware Version* dialog box displays (Figure 4-63 on page 4-75).

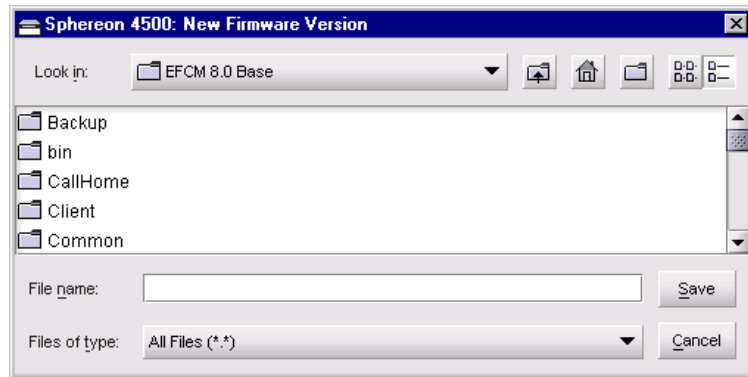


Figure 4-63 New Firmware Version Dialog Box

6. Select the desired firmware version file (downloaded in [step 1](#)) from the management server diskette drive or hard drive. Ensure the correct filename appears in the *File name* field and click *Save*. The *New Firmware Description* dialog box displays ([Figure 4-64](#)).

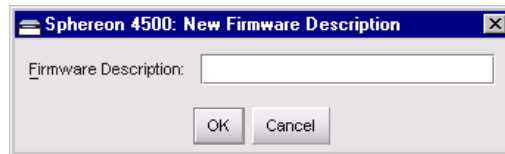


Figure 4-64 New Firmware Description Dialog Box

7. Enter a description (up to 24 characters) for the new firmware version. The description should include the installation date and text that uniquely identifies the firmware version. Click *OK*. The *File Transfer* message box displays ([Figure 4-65](#)). As the transfer progresses, a progress bar travels across the message box to show percent completion.

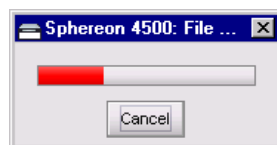


Figure 4-65 File Transfer Message Box

8. The *File Transfer* message box converts to a *Transfer Complete* message box, indicating the new firmware version is stored on the management server hard drive. Click *Close* to close the message box.
9. The new firmware version and associated description appear in the *Firmware Library* dialog box. Click *Close* to close the dialog box.
10. To send the firmware version to a switch, refer to [Download a Firmware Version to a Switch](#) below.

Download a Firmware Version to a Switch

To download a firmware version to a selected switch from the management server (Sphereon 4500 Element Manager application):

1. At the management server, open the SAN management application (SANavigator 4.0 or EFCM 8.0).
2. Before downloading firmware version *XX.YY.ZZ* to a switch, ensure version *XX.YY.ZZ* or higher of the SAN management application is running on the server.
 - a. Select the *About* option from the *Help* menu. The *About* dialog box displays the SAN management application version. Click *Close* to close the dialog box.
 - b. If required, install the correct version of the application. For instructions, refer to [Install or Upgrade Software](#) on page 4-87.
3. At the SAN management application's physical map, right-click the product icon representing the switch for which a firmware version is to be downloaded, then select *Element Manager* from the pop-up menu. The application opens.
4. As a precaution to preserve switch configuration information, perform the data collection procedure. For instructions, refer to [Collect Maintenance Data](#) on page 4-44.
5. Select the *Firmware Library* option from the *Maintenance* menu. The *Firmware Library* dialog box displays ([Figure 4-66](#) on page 4-77).

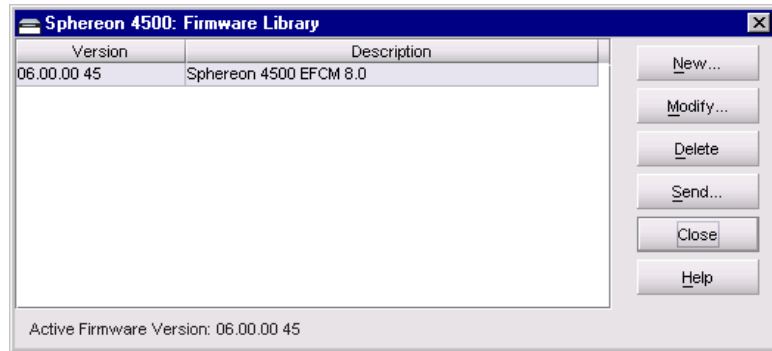


Figure 4-66 Firmware Library Dialog Box

6. Select (highlight) the firmware version to be downloaded and click *Send*. The send function verifies existence of certain switch conditions before the download process begins. If an error occurs, a message displays indicating the problem must be fixed before the firmware download. Conditions that terminate the process include:

- The firmware version is being installed to the switch by another user.
- The switch-to-management server link fails or times out.

If a problem occurs and a corresponding message displays, go to [MAP 0000: Start MAP](#) on page 3-6 to isolate the problem. If no error occurs, a *Warning* dialog box displays ([Figure 4-67](#)).

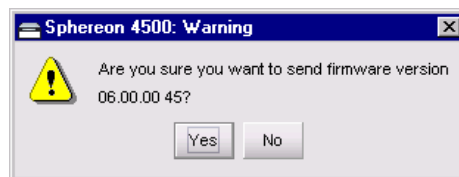


Figure 4-67 Warning Dialog Box

7. Click *Yes* to download the firmware version. The *Send Firmware* dialog box displays (Figure 4-68).

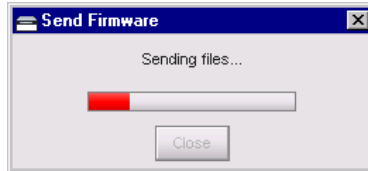


Figure 4-68 Send Firmware Dialog Box

8. The following occur during the download process:
 - a. As the download begins, a **Writing data to FLASH** message displays at the top of the dialog box for a few moments.
 - b. As the download progresses, a **Sending Files** message displays. This message remains as a progress bar travels across the dialog box to show percent completion of the download. The bar progresses to 100% when the last file is transmitted to the CTP card.
 - c. As the download finishes, a **Writing data to FLASH** message displays again for a few moments.
 - d. The switch performs an IPL, during which an **IPLing** message displays at the *Send Firmware* dialog box. In addition, the switch-to-management server Ethernet link drops momentarily and the following occur at the *Hardware View*:
 - As the network connection drops, the *Sphereon 4500 Status* table turns yellow, the *Status* field displays **No Link**, and the *State* field displays **Link Timeout**.
 - The status bar at the bottom of the window displays a grey square, indicating switch status is unknown.
 - Illustrated FRUs disappear, and appear again as the connection is re-established.
9. After the IPL, a **Send firmware complete** message displays at the *Send Firmware* dialog box. Click *Close* to close the dialog box.
10. Click *Close* to close the *Firmware Library* dialog box.

Manage Configuration Data

The Sphereon 4500 Element Manager application provides options to back up and restore the configuration file stored in nonvolatile random-access memory (NV-RAM) on the switch CTP card. The switch must be set offline prior to restoring the configuration file.

Configuration data in the file include:

- Switch identification data.
- Port configuration data.
- Switch and fabric operating parameters.
- Simple network management protocol (SNMP) configuration information.
- Zoning configuration information.

The SANpilot interface and the Element Manager application provide the option to reset the configuration file to factory default values. The switch must be set offline prior to resetting the configuration file.

Back Up the Configuration

To back up the switch configuration file to the management server using the Sphereon 4500 Element Manager application:

1. At the management server, open the SAN management application (SANavigator 4.0 or EFCM 8.0).
2. At the SAN management application's physical map, right-click the product icon representing the switch for which a configuration file is to be backed up, then select *Element Manager* from the pop-up menu. The application opens.
3. Select the *Backup & Restore Configuration* option from the *Maintenance* menu. The *Backup and Restore Configuration* dialog box displays ([Figure 4-69](#) on page 4-80).

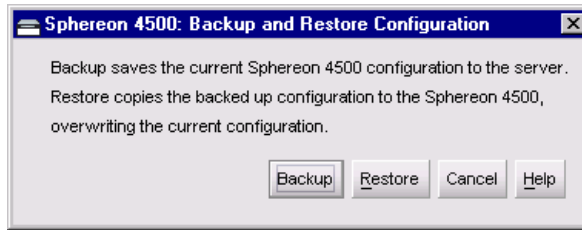


Figure 4-69 Backup and Restore Configuration Dialog Box

4. Click *Backup*. An *Information* dialog box displays, indicating the backup operation was initiated (Figure 4-70).

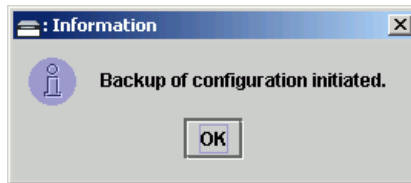


Figure 4-70 Information Dialog Box

5. Click *OK* to complete the backup operation and close the dialog box.

Restore the Configuration

To restore the switch configuration file from the management server using the Sphereon 4500 Element Manager application:

1. Notify the customer the switch is to be set offline. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the switch and sets attached FC-AL devices offline.
2. Set the switch offline. For instructions, refer to [Set the Switch Online or Offline](#) on page 4-48.
3. At the management server, open the SAN management application (SANavigator 4.0 or EFCM 8.0).
4. At the SAN management application's physical map, right-click the product icon representing the switch for which a configuration file is to be restored, then select *Element Manager* from the pop-up menu. The application opens.

5. Select the *Backup & Restore Configuration* option from the *Maintenance* menu. The *Backup and Restore Configuration* dialog box displays (Figure 4-71).

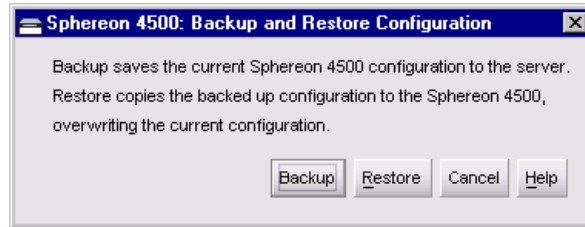


Figure 4-71 Backup and Restore Configuration Dialog Box

6. Click *Restore*. A *Warning* dialog box displays, indicating the existing configuration file is to be overwritten (Figure 4-72).

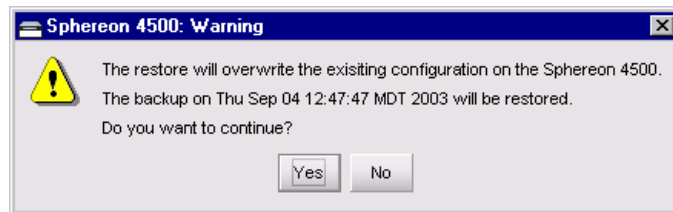


Figure 4-72 Warning Dialog Box

7. Click *Yes*. A *Restore* dialog box displays, indicating the restore operation is in progress (Figure 4-73).

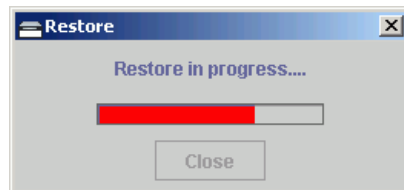


Figure 4-73 Information Dialog Box

8. When the operation finishes, the *Restore* dialog box displays a **Restore complete** message. Click *Close* to close the dialog box.

Reset Configuration Data (SANpilot Interface)

To reset switch data to the factory default settings from the SANpilot interface:

NOTE: When switch configuration data is reset to factory default values, all optional features are disabled.

1. Notify the customer the switch is to be set offline. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the switch and sets attached FC-AL devices offline.
2. Set the switch offline. For instructions, refer to [Set the Switch Online or Offline](#) on page 4-48.
3. When the SANpilot interface opens, the *View* panel and *Switch* page appear as the default. At the *View* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens with the *Switch* page displayed.
4. Click the *Reset Config* tab. The *Switch* page displays with the *Reset Config* tab selected ([Figure 4-74](#)).

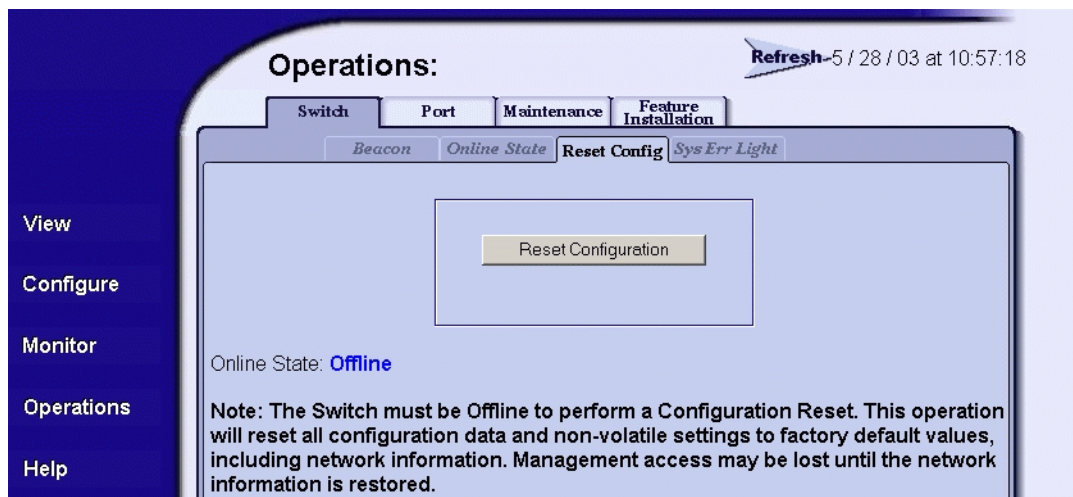


Figure 4-74 Operations Panel (Switch Page with Reset Config Tab)

5. Click *Reset Configuration*. A browser-specific message box displays (Figure 4-75).

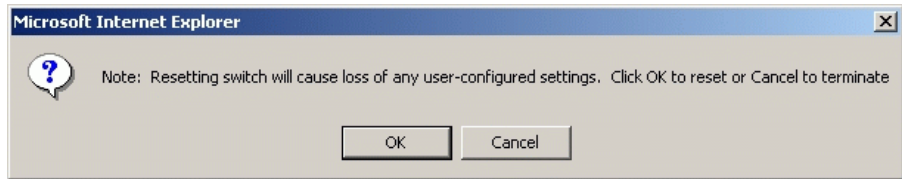


Figure 4-75 Browser-Specific Message Box

6. Click *OK* to reset the configuration. The message **Your changes have been successfully activated** appears.
7. The switch IP address resets to the default address of **10.1.1.10**.
 - If the configured IP address (prior to reset) was the same as the default address, the browser-to-switch Internet connection is not affected and the procedure is complete.
 - If the configured IP address (prior to reset) was not the same as the default address, the browser-to-switch Internet connection drops and the SANpilot session is lost. Continue to the next step.
8. To change the switch IP address and restart the SANpilot interface, refer to [Configure Network Information](#) on page 2-24. To restart the SANpilot interface using the default IP address of **10.1.1.10**:
 - a. At the browser, enter the default IP address of **10.1.1.10** as the Internet URL. The *Enter Network Password* dialog box displays.
 - b. Type the default user name and password.

NOTE: The default user name is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

- c. Click *OK*. The SANpilot interface opens with the *View* panel open and the *Switch* page displayed. The procedure is complete.

Reset Configuration Data (Management Server)

To reset switch data to the factory default settings from the management server (Sphereon 4500 Element Manager application):

NOTE: When switch configuration data is reset to factory default values, all optional features are disabled.

1. Notify the customer the switch is to be set offline. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the switch and sets attached FC-AL devices offline.
2. At the management server, open the SAN management application (SANavigator 4.0 or EFCM 8.0).
3. Set the switch offline. For instructions, refer to [Set the Switch Online or Offline](#) on page 4-48.
4. At the SAN management application's physical map, right-click the product icon representing the switch for which a configuration file is to be reset to factory default settings, then select *Element Manager* from the pop-up menu. The application opens.
5. Select the *Reset Configuration* option from the *Maintenance* menu. The *Reset Configuration* dialog box displays ([Figure 4-76](#)).

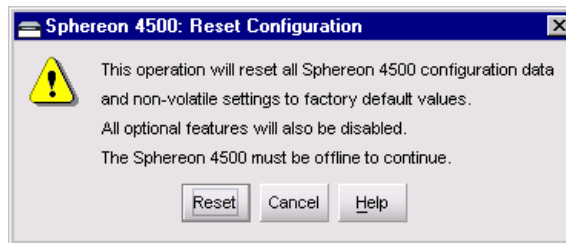


Figure 4-76 Reset Configuration Dialog Box

6. Click *Reset* to initiate the reset operation and close the dialog box.
7. The switch IP address resets to the default address of **10.1.1.10**.
 - If the configured IP address (prior to reset) was the same as the default address, the switch-to-management server Ethernet link is not affected and the procedure is complete.

- If the configured IP address (prior to reset) was not the same as the default address, the switch-to-management server Ethernet link drops and server communication is lost. Continue to the next step.
8. To change the switch IP address and restart the management server session, go to [step 10](#).
 9. To restart a management server session using the default IP address of **10.1.1.10**:
 - a. Close the Sphereon 4500 Element Manager application and return to the SAN management application.
 - b. A grey square with a yellow exclamation mark appears adjacent to the icon representing the reset switch, indicating switch is not communicating with the management server.
 - c. At the SAN management application, select the *Setup* option from the *Discover* menu. The *Discover Setup* dialog box displays ([Figure 4-77](#)).

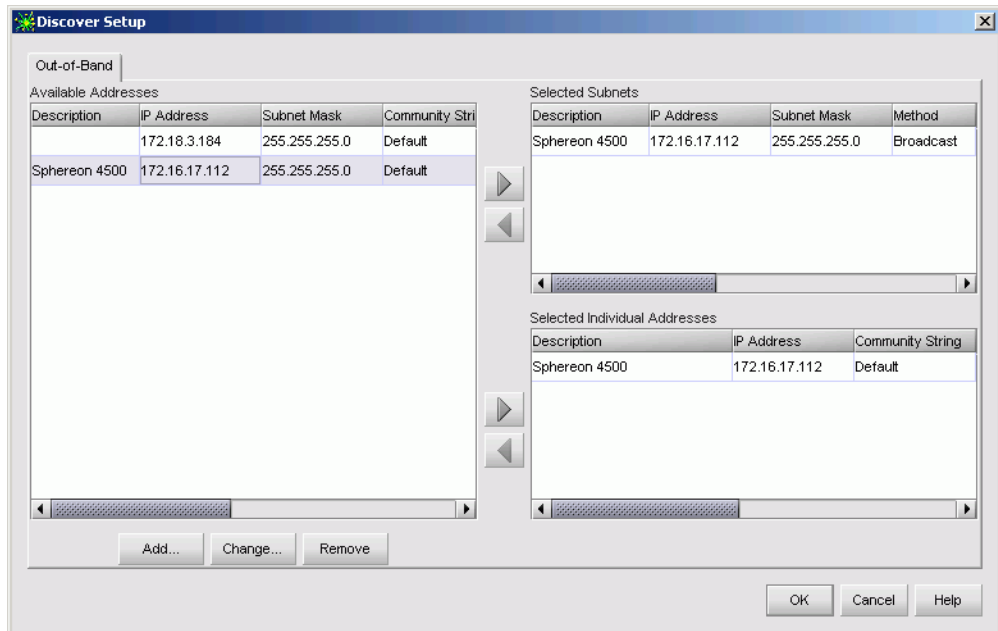


Figure 4-77 Discover Setup Dialog Box

- d. Select (highlight) the entry representing the reset switch in the *Available Addresses* window and click *Change*. The *Domain Information* dialog box displays (Figure 4-78).

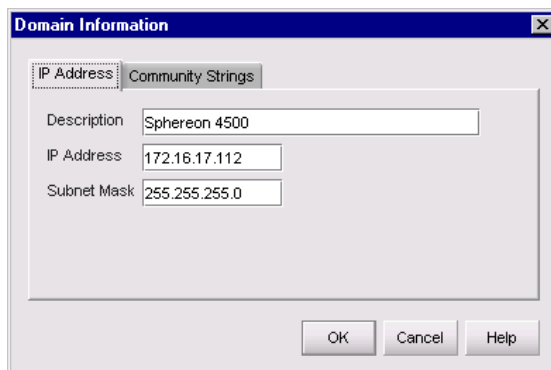


Figure 4-78 Domain Information Dialog Box

- e. Type **10.1.1.10** in the *IP Address* field and click *OK*. Entries at the *Discover Setup* dialog box reflect the new IP address.
- f. At the *Discover Setup* dialog box, click *OK*. Switch-to-management server communication is restored and the procedure is complete.
10. Change the switch IP address and restart the management server session as follows:
- A grey square with a yellow exclamation mark appears adjacent to the icon representing the reset switch, indicating switch is not communicating with the management server.
 - Delete the icon representing the reset switch. At the SAN management application, select the *Setup* option from the *Discover* menu. The *Discover Setup* dialog box displays (Figure 4-77 on page 4-85).
 - Select (highlight) the entry representing the reset switch in the *Available Addresses* window and click *Remove*.
 - At the *Discover Setup* dialog box, click *OK*. The switch is no longer defined to the management server.
 - Change a switch's IP address through the maintenance port at the rear of the switch. For instructions, refer to [Task 5: Configure Switch Network Information \(Optional\)](#) on page 2-41.

- e. Identify the switch to the SAN management application. For instructions, refer to [Task 13: Configure the Switch to the Management Application](#) on page 2-76.
- f. Switch-to-management server communication is restored and the procedure is complete.

Install or Upgrade Software

This section describes the procedure to install or upgrade the SAN management application at the management server. The application includes the Sphereon 4500 Element Manager application.

The SAN management application shipped with the switch is provided on the *EFC Management Applications* CD-ROM. Subsequent software versions for upgrading the switch are provided to customers through an *EFC Management Applications* CD-ROM or through McDATA's Internet home page.

NOTE: When installing or upgrading a software version, follow all procedural information contained in release notes or EC instructions that accompany the software version. This information supplements information provided in this general procedure.

To install or upgrade the SAN management application and associated applications to the server:

1. At the management server, close all SAN management sessions (local and remote) and exit all applications.
2. To install the new software version from the *EFC Management Applications* CD-ROM, go to [step 4](#).
3. To obtain a new software version from the McDATA File Center:
 - a. At a PC with Internet access, open the File Center home page ([Figure 4-79](#) on page 4-88). The URL is <http://central.mcdata.com>.

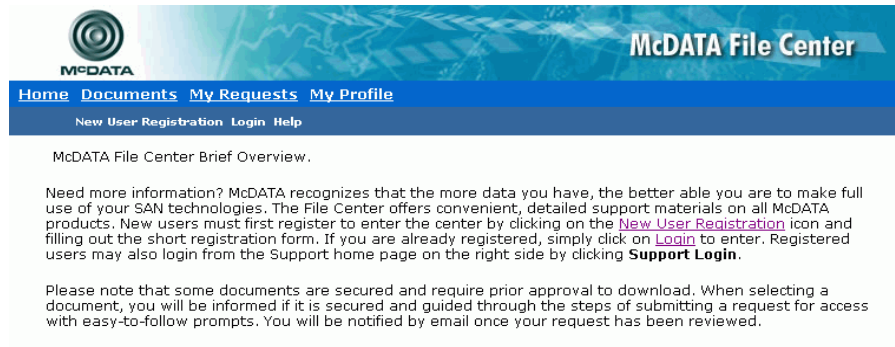


Figure 4-79 McDATA File Center Home Page

- b. Select (click) the *Login* option at the top of the home page. The *Login* page displays (Figure 4-41 on page 4-61).
- c. Type the user name and password (assigned and registered while performing *Task 24: Register with the McDATA File Center* on page 2-127) and click *Login*. The *Welcome* page displays.
- d. Select (click) the *Documents* option at the top of the page. The *Find Documents* page displays (Figure 4-80).


Click the check boxes on the left of each search option to include it in the search criteria. Then fill in any requested data for that search criteria. This helps narrow the search to give you more accurate search results.

Find documents where

<input checked="" type="checkbox"/>	Category is one or more of the following	<div> <div>ES 3xxx Firmware</div> <div>Technical News Letters</div> <div>EOS Release Notes</div> <div>EFCM Software</div> </div>
<input type="checkbox"/>	And the title contains one or more of the following words	<input type="text"/>
<input type="checkbox"/>	And the description contains one or more of the following words	<input type="text"/>
		<input type="button" value="search"/>

Figure 4-80 McDATA File Center (Find Documents Page)

- e. Select (highlight) the *EFCM Software* option at the list box and click *Search*. The *Documents Match* page displays (Figure 4-81) with a list of software available for download.



McDATA File Center

Home Documents My Requests My Profile

Search New Documents By Category

The following documents match your search criteria.

Showing 1-3 of 3 items.



Status	Action	Size	Title	Description	Online Date	Offline Date
	Add To Request	145942k	EFCM V. 7.01	This can only be installed on McDATA supplied hardware. It supports all current products, and is required to be used with EOS 5.01	05/01/2003	

Figure 4-81 McDATA File Center (Documents Match Page)

- f. Authorization to download a software version requires approval from the McDATA Solution Center. In the *Action* column adjacent to the desired software version, click *Add to Request*. The *Current Request* page displays (Figure 4-82).



McDATA File Center

Home Documents My Requests My Profile

History Current

Current Request: Not Yet Submitted

Action	Title	Description
Remove	EFCM V. 7.01	This can only be installed on McDATA supplied hardware. It supports all current products, and is required to be used with EOS 5.01

Submit Request

Figure 4-82 McDATA File Center (Current Request Page)

- g. Click *Submit Request*. The *Request Submitted* page displays and the request for approval is e-mailed to the McDATA Solution Center. Wait five to ten minutes for a response from McDATA, then select (click) the *My Requests* option at the top of the page. The *Request History* page displays (Figure 4-83) with the approved request.



The screenshot shows the McDATA File Center interface. At the top is the McDATA logo and the title 'McDATA File Center'. Below this is a navigation bar with links: Home, Documents, My Requests, and My Profile. Under 'My Requests', there are sub-links for 'History' and 'Current'. The main content area is titled 'Request History' and indicates 'Showing 1-2 of 2 items.' Below this is a table with request details.

Status	Action	Title	Description	Reviewed On
Approved	Download	EFCM V. 7.01	This can only be installed on McDATA supplied hardware. It supports all current products, and is required to be used with EOS 5.01	05/15/2003

Figure 4-83 McDATA File Center (Request History Page)

- h. In the *Action* column adjacent to the approved request for the software version, click *Download*. The *File Download* dialog box displays (Figure 4-84).

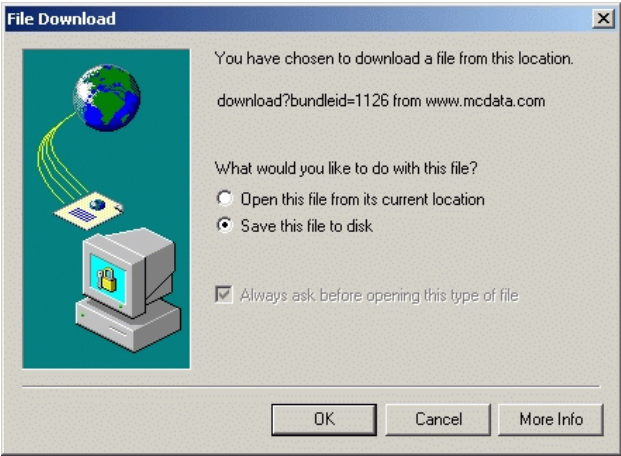


Figure 4-84 File Download Dialog Box

- i. Select the *Save this file to disk* radio button and click *OK*. The *Save As* dialog box appears (Figure 4-85).

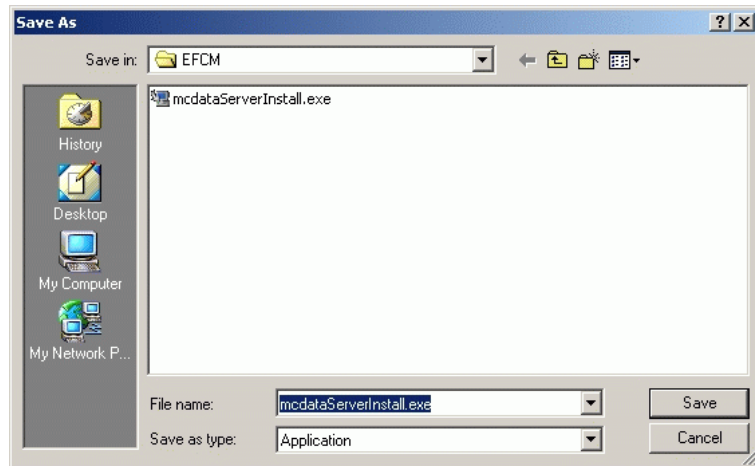


Figure 4-85 Save As Dialog Box

- j. At the *Save As* dialog box, ensure the correct directory path is specified at the *Save in* field, the correct file is specified in the *File name* field, and click *Save*.
- k. A *Download* dialog box displays, showing the estimated time remaining to complete the download process. When the process finishes, the dialog box changes to a *Download complete* dialog box (Figure 4-86).

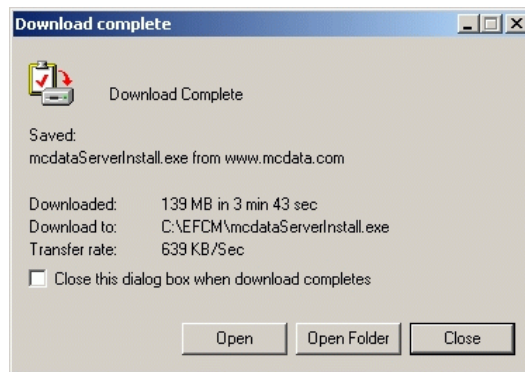


Figure 4-86 Download Complete Dialog Box

- l. Click *Close* to close the dialog box. The new firmware version is downloaded and saved to the PC hard drive.
 - m. At the PC, close the Internet session.
 - n. Transfer the firmware version file from the PC to the rack-mount management server by diskette, CD-ROM, or other electronic means.
 - o. Go to [step 5](#).
4. Insert the *EFC Management Applications* CD-ROM into the CD-ROM drive of the management server.
 5. At the management server's Windows 2000 desktop, click *Start* at the left side of the task bar, then select the *Run* option. The *Run* dialog box displays ([Figure 4-87](#)).

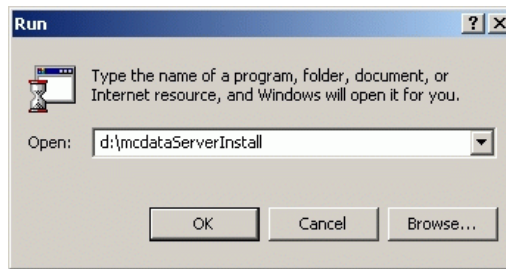


Figure 4-87 Run Dialog Box

6. At the *Run* dialog box, type **D:\mcdataServerInstall** in the *Open* field.
7. Click *OK*. A series of message boxes appear as the *InstallAnywhere* third-party application prepares to install the SAN management software, followed by the *McDATA EFC Management Applications* dialog box ([Figure 4-88](#) on page 4-93).

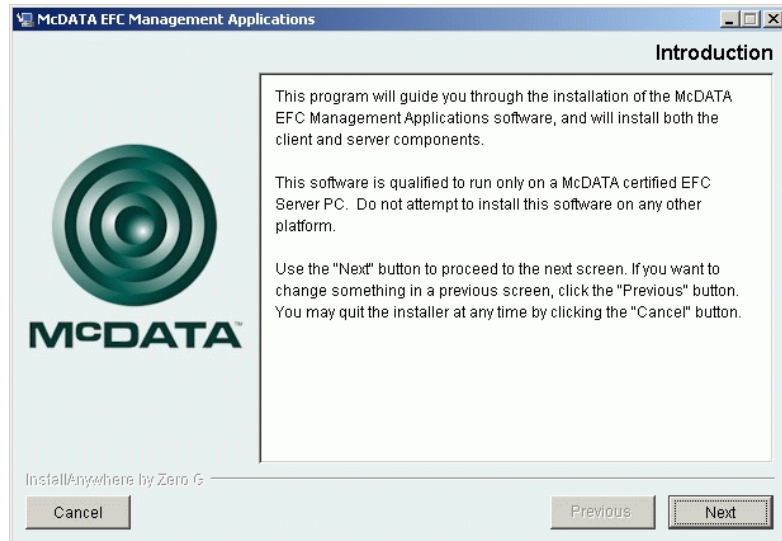


Figure 4-88 McDATA EFC Management Applications Dialog Box

8. Follow the online instructions for the *InstallAnywhere* program. Click *Next*, *Install*, or *Done* as appropriate.
9. Power off and reboot the rack-mount management server.
 - a. At the Windows 2000 desktop, click *Start* at the left side of the task bar (bottom of the desktop), then select *Shut Down*. The *Shut Down Windows* dialog box displays.
 - b. Select the *Restart* option from the list box and click *OK*. The management server powers down and restarts. During the reboot process the LAN connection between the server and browser-capable PC drops momentarily, and the TightVNC viewer displays a network error.
 - c. After the management server reboots, click *Login again*. The *VNC Authentication* screen displays.
 - d. Type the default password and click *OK*. The *Welcome to Windows* dialog box displays.

NOTE: The default TightVNC viewer password is **password**.

- e. Click the **Send Ctrl-Alt-Del** button at the top of the window to log on to the management server desktop. The *Log On to Windows* dialog box displays.

NOTE: Do not simultaneously press the **Ctrl**, **Alt**, and **Delete** keys. This action logs the user on to the browser-capable PC, not the rack-mount management server.

- f. Type the default Windows 2000 user name and password and click **OK**. The management server's Windows 2000 desktop opens and the *SANavigator Log In* or *EFCM Log In* dialog box displays (Figure 4-89).

NOTE: The default Windows 2000 user name is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

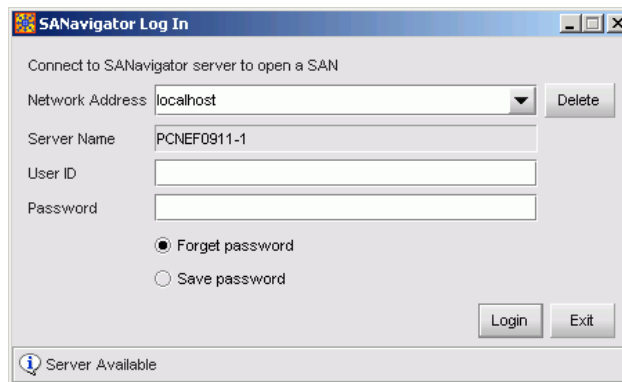


Figure 4-89 SANavigator Log In or EFCM Log In Dialog Box

- g. Type the SAN management application default user ID and password and select a server or IP address from the *Network Address* drop-down list.

NOTE: The default SAN management application user ID is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

- h. Click *Login*. The application opens and the SANavigator or EFCM main window appears.

This chapter describes removal and replacement procedures (RRPs) used by authorized service representatives for all Sphereon 4500 Fabric Switch field-replaceable units (FRUs). Do not remove a switch FRU until a failure is isolated to that FRU. If fault isolation was not performed, refer to *MAP 0000: Start MAP* on page 3-6.

Procedural Notes

The following procedural notes are referenced in applicable removal and replacement procedures. The notes do not necessarily apply to all procedures in the chapter.

1. Before removing a FRU, read the removal and replacement procedures for that FRU carefully and thoroughly to familiarize yourself with the procedures and reduce the possibility of problems or customer down time.
2. When performing procedures described in this chapter, follow all **DANGER** and **ATTENTION** statements, and statements listed in the preface of this manual.
3. After completing steps of a detailed procedure that is referenced from another procedure, return to the initial (referencing) procedure and continue to the next step of that procedure.
4. After completing a replacement procedure, clear the event code reporting the failure and the event code reporting the recovery from the *Event Log* (at the SANpilot interface or management server), and extinguish the amber system error (**ERR**) light-emitting diode (LED) at the switch front panel.

Remove and Replace FRUs

This section describes procedures to remove and replace concurrent switch FRUs, along with tools required to perform each procedure. Concurrent FRUs are removed and replaced while the switch is powered on and operational. Refer to [Chapter 6, *Illustrated Parts Breakdown*](#) for FRU locations and part numbers.

[Table 5-1](#) lists concurrent FRUs that are removed and replaced while the switch is powered on and operational. The table also lists ESD precautions (yes or no) for each FRU, and references the page number of the removal and replacement procedure.

Table 5-1 Concurrent FRUs

Concurrent FRU Name	ESD Precaution Requirement	Page
Small form factor pluggable (SFP) optical transceiver	No	5-2
Redundant power supply (with internal cooling fans)	No	5-6

RRP 1: SFP Optical Transceiver

Use the following procedures to remove or replace an SFP optical transceiver from the front of the switch chassis. A list of tools required is provided.

Tools Required

The following tools are required to perform these procedures.

- Door key with 5/16-inch socket (provided with the FC-512 Fabricenter equipment cabinet).
- Protective cap (provided with the fiber-optic jumper cable).
- Loopback plug (provided with the switch).
- Fiber-optic cleaning kit.

Removal

To remove an SFP optical transceiver:

1. Notify the customer that the port with the defective transceiver will be blocked. Ensure the customer's system administrator sets the attached device offline.
2. If the switch is installed as part of a stand-alone configuration, go to [step 3](#). If the switch is rack-mounted, perform one of the following:

- If the switch is installed in a McDATA FC-512 Fabriccenter equipment cabinet, insert the 5/16-inch door tool into the socket hole at the right top of the front door. Turn the tool counter-clockwise to unlock and open the door.
 - If the switch is installed in a customer-supplied equipment cabinet, unlock and open the cabinet front door as directed by the customer representative.
3. Identify the defective port transceiver from:
 - The illuminated amber LED adjacent to the port.
 - At the SANpilot interface, failure information associated with the port at the *Port Properties* page of the *View* panel.
 - At the management server (Sphereon 4500 Element Manager application), failure information associated with the port at the *Hardware View*, *Port List View*, or *Port Properties* dialog box.
 4. Block communication to the port. Refer to [Block or Unblock a Port](#) on page 4-51 for instructions.
 5. Disconnect the fiber-optic jumper cable from the port:
 - a. Pull the keyed LC connector free from the port's optical transceiver.
 - b. Place a protective cap over the jumper cable connector.
 6. The optical transceiver has a wire locking bale to secure the transceiver in the port receptacle and to assist in removal. The locking bale rotates up or down, depending on the transceiver manufacturer and port location (top row, odd-numbered ports **1** through **23**, or bottom row even-numbered ports **0** through **22**).
 - a. Disengage the locking mechanism by rotating the wire locking bale up or down 90 degrees as shown in part (A) of [Figure 5-1](#) on page 5-4.
 - b. Grasp the wire locking bale and pull the transceiver from the port receptacle as shown in part (B) of [Figure 5-1](#) on page 5-4.

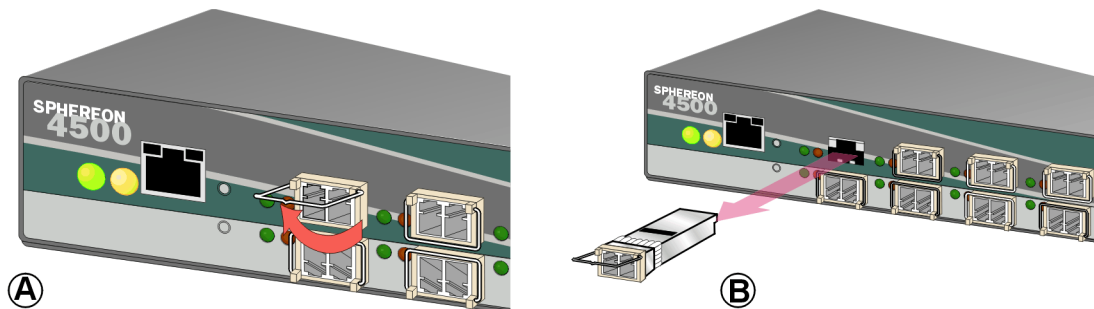


Figure 5-1 SFP Optical Transceiver Removal and Replacement

7. Perform one of the following to inspect the *Event Log*:
 - If at a web browser connected to the SANpilot interface, click the *Log* tab at the *Monitor* panel. The *Event Log* displays. An event code **513** (SFP optics hot-removal completed) appears.
 - If at the management server, open the *Hardware View*, click *Logs*, and select *Event Log*. The *Event Log* displays. An event code **513** (SFP optics hot-removal completed) appears.

Replacement

To replace an SFP optical transceiver:

1. Remove the replacement transceiver from its packaging.
2. Insert the transceiver into the port receptacle, then engage the locking mechanism by rotating the wire locking bale up or down 90 degrees as shown in [Figure 5-1](#).
3. Perform an external loopback test on the port. Refer to [Perform Port Diagnostic Loopback Tests](#) on page 4-38 for instructions. If the test fails, go to [MAP 0000: Start MAP](#) on page 3-6 to isolate the problem.
4. Reconnect the fiber-optic jumper cable:
 - a. Remove the protective cap from the cable connector and the protective plug from the port's optical transceiver. Store the cap and plug in a suitable location for safekeeping.
 - b. Clean the jumper cable and transceiver connectors. Refer to [Clean Fiber-Optic Components](#) on page 4-54 for instructions.

- c. Insert the keyed LC cable connector into the port's optical transceiver.
5. Ensure the amber LED adjacent to the port transceiver is extinguished. If the amber LED is illuminated, go to [MAP 0000: Start MAP](#) on page 3-6 to isolate the problem.
6. Perform one of the following to inspect the *Event Log*:
 - If at a web browser connected to the SANpilot interface, click the *Log* tab at the *Monitor* panel. The *Event Log* displays. Ensure an event code **510** (SFP optics hot-insertion initiated) appears. If the event code does not appear, go to [MAP 0000: Start MAP](#) on page 3-6 to isolate the problem.
 - If at the management server, open the *Hardware View*, click *Logs*, and select *Event Log*. The *Event Log* displays. Ensure an event code **510** (SFP optics hot-insertion initiated) appears. If the event code does not appear, go to [MAP 0000: Start MAP](#) on page 3-6 to isolate the problem.
7. Perform one of the following to verify port operation:
 - If at a web browser connected to the SANpilot interface, open the *Switch* tab at the *View* panel and:
 - a. Ensure no amber LEDs illuminate that indicate a port failure.
 - b. Click the graphic representing the port with the replacement transceiver to open the *Port Properties* tab. Verify port and port technology information is correct.
 - c. If a problem is indicated, go to [MAP 0000: Start MAP](#) on page 3-6 to isolate the problem.
 - If at the management server, open the *Hardware View* and:
 - a. Ensure no alert symbols appear that indicate a port failure (yellow triangle or red diamond).
 - b. Double-click the graphic representing the port with the replacement transceiver to open the *Port Properties* dialog box. Verify port information is correct.
 - c. Right-click the graphic representing the port with the replacement transceiver and select *Port Technology* from the menu. The *Port Technology* dialog box displays. Verify port technology information is correct.

- d. If a problem is indicated, go to [MAP 0000: Start MAP](#) on page 3-6 to isolate the problem.
8. Restore communication to the port with the replacement transceiver as directed by the customer. Refer to [Block or Unblock a Port](#) on page 4-51 for instructions. Inform the customer the port is available.
9. Perform one of the following to clear the system error (ERR) LED on the switch front bezel:
 - If at a web browser connected to the SANpilot interface:
 - a. Click the *Switch* tab at the *Operations* panel. The *Operations* panel opens with the *Switch* page displayed.
 - b. Click the *Sys Err Light* tab. The *Switch* page displays with the *Sys Err Light* tab selected. A **System Error Light is ON** message displays on the page.
 - c. Click *Clear Light*.
 - If at the management server, open the *Hardware View* and:
 - a. Right-click the front panel bezel graphic (away from a FRU) to open a menu.
 - b. Click the *Clear System Error Light* menu selection.
10. If necessary, close and lock the equipment cabinet door.

RRP 2: Redundant Power Supply

Use the following procedures to remove or replace a redundant power supply (with internal cooling fans) from the rear of the switch chassis. A list of tools required is provided.

Tools Required

A door key with 5/16-inch socket (provided with the FC-512 Fabricenter equipment cabinet) is required to perform these procedures.

Removal

To remove a redundant power supply:

1. If the switch is installed as part of a stand-alone configuration, go to [step 2](#). If the switch is rack-mounted, perform one of the following:
 - If the switch is installed in a McDATA FC-512 Fabricenter equipment cabinet, insert the 5/16-inch door tool into the socket hole at the right top of the front door. Turn the tool counter-clockwise to unlock and open the door.

- If the switch is installed in a customer-supplied equipment cabinet, unlock and open the cabinet front door as directed by the customer representative.
2. Identify the defective power supply from:
 - The illuminated amber LED on the FRU.
 - At the SANpilot interface, failure information associated with the power supply at the *FRU Properties* page of the *View* panel.
 - At the management server (Sphereon 4500 Element Manager application), failure information associated with the power supply at the *Hardware View* or *FRU List View*.
 3. Disconnect the AC power cord from the power supply.



DANGER

Disconnect the power cords.

4. Disengage and remove the power supply as follows:
 - a. Disengage the locking mechanism by rotating both finger handles outward by 90 degrees as shown in part (A) of [Figure 5-2](#).

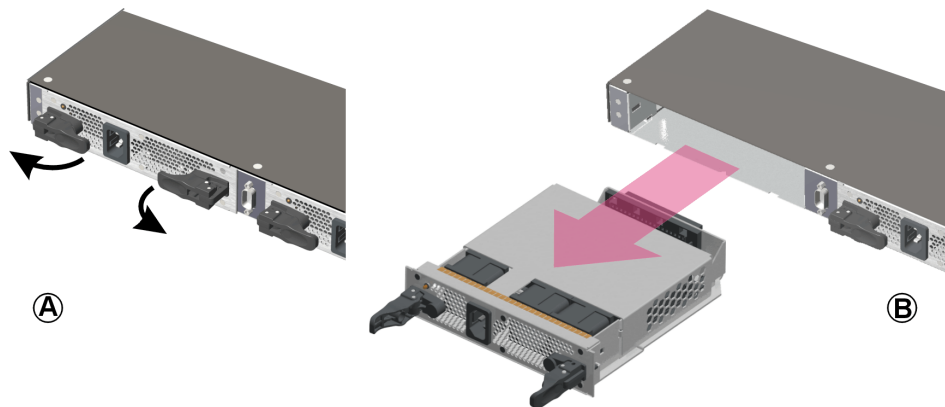


Figure 5-2 Redundant Power Supply Removal and Replacement

- b. Use the finger handles to pull the power supply out of the switch chassis as shown in part (B) of [Figure 5-2](#) on page 5-7. Support the power supply as it is pulled from the chassis.
5. Perform one of the following to inspect the *Event Log*. Note that multiple events appear because the power supply contains three internal cooling fans.
 - If at a web browser connected to the SANpilot interface, click the *Log* tab at the *Monitor* panel. The *Event Log* displays. The following event codes appear:
 - **200** - Power supply AC voltage failure (recorded when AC power is disconnected).
 - **300** - A cooling fan propeller has failed (first fan).
 - **301** - A cooling fan propeller has failed (second fan).
 - **302** - A cooling fan propeller has failed (third fan).
 - **206** - Power supply removed.
 - If at the management server, open the *Hardware View*, click *Logs*, and select *Event Log*. The *Event Log* displays. The following event codes appear:
 - **200** - Power supply AC voltage failure (recorded when AC power is disconnected).
 - **300** - A cooling fan propeller has failed (first fan).
 - **301** - A cooling fan propeller has failed (second fan).
 - **302** - A cooling fan propeller has failed (third fan).
 - **206** - Power supply removed.

Replacement

To replace a redundant power supply:

1. Remove the replacement power supply from its shipping container.
2. Inspect the rear of the power supply for bent or broken connector pins that may have been damaged during shipping. If any pins are damaged, obtain a new power supply.
3. Position the power supply in the rear of the switch chassis as shown in part (B) of [Figure 5-2](#) on page 5-7. Ensure the finger handles are disengaged and rotated 90 degrees outward.

- a. While supporting the power supply with one hand, insert it into the switch chassis.
 - b. Firmly push the power supply into the chassis. Rotate the finger handles 90 degrees inward to seat the power supply and engage the connector pins. Ensure the faceplate is flush with the chassis cutout.
4. Connect the AC power cord to the power supply and to a facility power source.
 5. Wait several seconds, then inspect the power supply to ensure the amber LED is extinguished. If the LED is illuminated, go to [MAP 0000: Start MAP](#) on page 3-6 to isolate the problem.
 6. Perform one of the following to inspect the *Event Log*:
 - If at a web browser connected to the SANpilot interface, click the *Log* tab at the *Monitor* panel. The *Event Log* displays. Ensure the following event codes appear. If the event codes do not appear, go to [MAP 0000: Start MAP](#) on page 3-6 to isolate the problem.
 - 207 - Power supply installed.
 - 313 - A cooling fan propeller has recovered (first fan).
 - 314 - A cooling fan propeller has recovered (second fan).
 - 315 - A cooling fan propeller has recovered (third fan).
 - 203 - Power supply AC voltage recovery.
 - If at the management server, open the *Hardware View*, click *Logs*, and select *Event Log*. The *Event Log* displays. Ensure the following event codes appear. If the event codes do not appear, go to [MAP 0000: Start MAP](#) on page 3-6 to isolate the problem.
 - 207 - Power supply installed.
 - 313 - A cooling fan propeller has recovered (first fan).
 - 314 - A cooling fan propeller has recovered (second fan).
 - 315 - A cooling fan propeller has recovered (third fan).
 - 203 - Power supply AC voltage recovery.

7. Perform one of the following to verify power supply operation:
 - If at a web browser connected to the SANpilot interface, open the *Switch* tab at the *View* panel and ensure no amber LEDs illuminate that indicate a power supply failure. If a problem is indicated, go to [MAP 0000: Start MAP](#) on page 3-6 to isolate the problem.
 - If at the management server, open the *Hardware View* and observe the power supply graphic to ensure no alert symbols appear that indicate a failure (yellow triangle or red diamond). If a problem is indicated, go to [MAP 0000: Start MAP](#) on page 3-6 to isolate the problem.
8. Perform the data collection procedure. Refer to [Collect Maintenance Data](#) on page 4-44 for instructions.
9. Perform one of the following to clear the system error (ERR) LED on the switch front bezel:
 - If at a web browser connected to the SANpilot interface:
 - a. Click the *Switch* tab at the *Operations* panel. The *Operations* panel opens with the *Switch* page displayed.
 - b. Click the *Sys Err Light* tab. The *Switch* page displays with the *Sys Err Light* tab selected. A **System Error Light is ON** message displays on the page.
 - c. Click *Clear Light*.
 - If at the management server, open the *Hardware View* and:
 - a. Right-click the front panel bezel graphic (away from a FRU) to open a menu.
 - b. Click the *Clear System Error Light* menu selection.
10. If necessary, close and lock the equipment cabinet door.

This chapter provides an illustrated parts breakdown for Sphereon 4500 Fabric Switch field-replaceable units (FRUs). Exploded-view assembly drawings are provided for:

- Front-accessible FRUs.
- Rear-accessible FRUs.
- Miscellaneous parts.
- Power cords and receptacles.

Exploded-view illustrations portray the switch disassembly sequence for clarity. Illustrated FRUs are numerically keyed to associated tabular parts lists. The parts lists also include McDATA part numbers, descriptions, and quantities.

Front-Accessible FRUs

Figure 6-1 illustrates front-accessible FRUs. Table 6-1 is the associated FRU parts list. The table includes reference numbers to Figure 6-1, FRU part numbers, descriptions, and quantities.

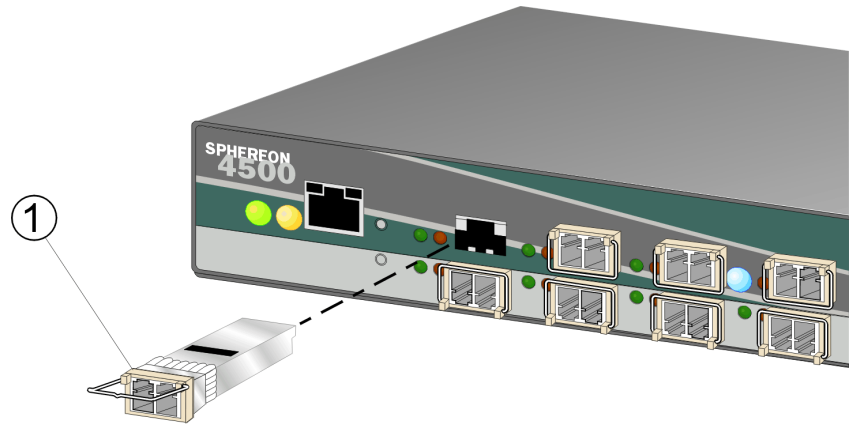


Figure 6-1 Front-Accessible FRUs

Table 6-1 Front-Accessible FRU Parts List

Ref.	Part Number	Description	Qty.
6-1	002-002579-002	Switch, Spheron 4500, base assembly	Reference
-1	803-000054-395	Transceiver, optical, SFP, shortwave laser, LC connector, 1.0625 Gbps	0 to 24
-1	803-000064-395	Transceiver, optical, SFP, shortwave laser, LC connector, 2.125 Gbps	0 to 24
-1	803-000056-313	Transceiver, optical, SFP, longwave laser, LC connector, 10 km, 1.0625 Gbps	0 to 24
-1	803-000065-313	Transceiver, optical, SFP, longwave laser, LC connector, 10 km, 2.125 Gbps	0 to 24
-1	803-000066-313	Transceiver, optical, SFP, longwave laser, LC connector, 20 km, 2.125 Gbps	0 to 24
-1	803-000067-313	Transceiver, optical, SFP, longwave laser, LC connector, 35 km, 2.125 Gbps	0 to 24

Rear-Accessible FRUs

Figure 6-2 illustrates rear-accessible FRUs. Table 6-2 is the associated FRU parts list. The table includes reference numbers to Figure 6-2, FRU part numbers, descriptions, and quantities.

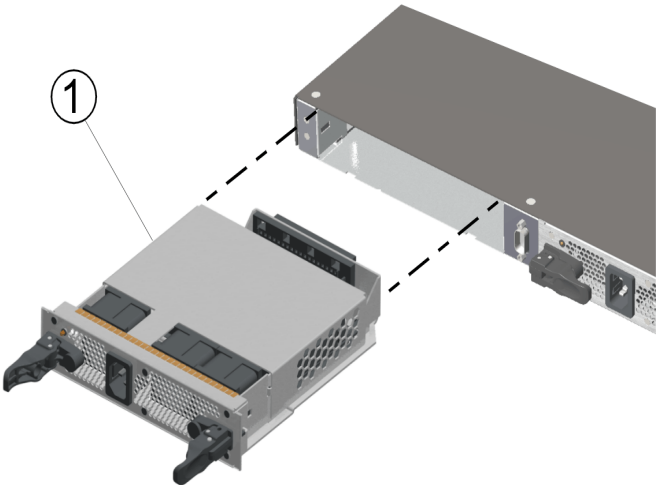


Figure 6-2 Rear-Accessible FRUs

Table 6-2 Rear-Accessible FRU Parts List

Ref.	Part Number	Description	Qty.
6-1	002-002579-002	Switch, Sphereon 4500, base assembly	Reference
-1	721-000072-201	Power supply assembly, 70-watt rated, 3.3 VDC, 5 VDC, and 12 VDC (includes three fan assemblies as part of the FRU)	2

Miscellaneous Parts

Figure 6-3 illustrates miscellaneous parts. Table 6-3 is the associated parts list. The table includes reference numbers to Figure 6-3, part numbers, descriptions, and quantities.

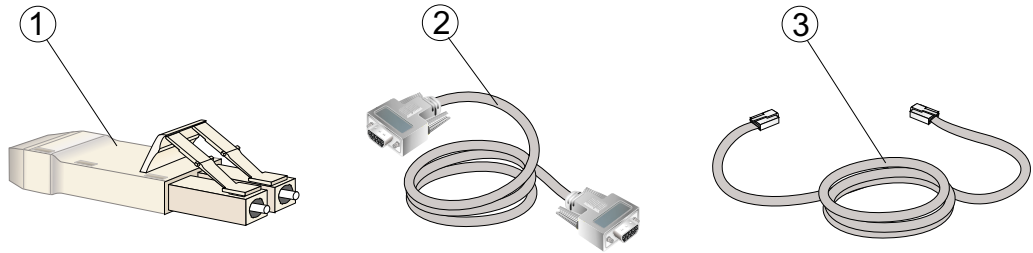


Figure 6-3 Miscellaneous Parts

Table 6-3 Miscellaneous Parts List

Ref.	Part Number	Description	Qty.
-1	803-000057-000	Plug, loopback, LC connector, multimode, 50/125 micron (#1148)	1
-1	803-000057-001	Plug, loopback, LC connector, singlemode, 9/125 micron (#1149)	1
-2	801-000039-000	Cable, null modem, DB9F-DB9F connector	1
-3	801-000035-010	Cable, Ethernet, 10-foot	1

Power Cords and Receptacles

Figure 6-4 illustrates optional power cords and receptacles. Table 6-4 on page 6-6 is the associated parts list. The table includes reference numbers to Figure 6-4, feature numbers, and descriptions.


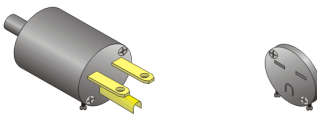
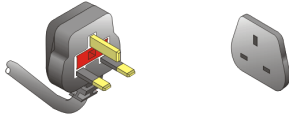
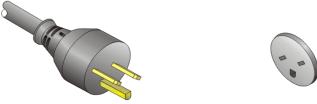
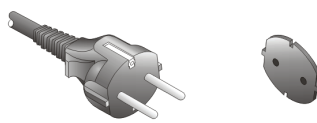

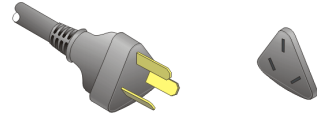
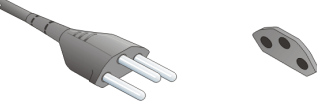
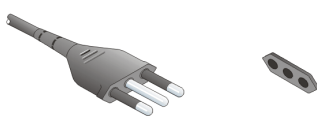
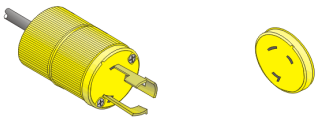


1		7, 11,15	
2		8	
3		9	
4		10	
5		12, 13,14	
6		16	

Figure 6-4 Power Cords and Receptacles

Table 6-4 Power Cord and Receptacle List

Ref.	Part Number	Description	Feature
-1	806-000001-000	Power cord, AC, North America NEMA 5-15P straight, 125 volts, 10 amps, 3.0 meters Receptacle: NEMA 5-15R	1010
-2	806-000004-001	Power cord, AC, United Kingdom BS 1363 right angle, 250 volts, 10 amps, 2.8 meters Receptacle: BS 1363	1012
-3	806-000005-001	Power cord, AC, European Community CEE 7/7 straight, 250 volts, 10 amps, 2.5 meters Receptacle: CEE 7	1013
-4	806-000006-001	Power cord, AC, Australia AS 3112 straight, 250 volts, 10 amps, 2.8 meters Receptacle: AS 3112	1014
-5	806-000027-000	Power cord, AC, Italy, Chile, Libya, and Ethiopia CEI 23-16/VII straight, 250 volts, 10 amps, 2.8 meters Receptacle: CEI 23-16/VII	1021
-6	806-000029-000	Power cord, AC, Israel SI-32 right angle, 250 volts, 15 amps, 2.8 meters Receptacle: SI-32	1022
-7	806-000030-000	Power cord, AC, Thailand, Philippines, Taiwan, Bolivia, and Peru NEMA 6-15P straight, 250 volts, 15 amps, 2.8 meters Receptacle: NEMA 6-15R	1023
-8	806-000033-000	Power cord, AC, Denmark Afsnit 107-2-D1 straight, 250 volts, 10 amps, 2.8 meters Receptacle: Afsnit 107-2-D1	1024
-9	806-000034-000	Power cord, AC, South Africa, Burma, Pakistan, India, and Bangladesh BS 546 Type, right angle, 250 volts, 15 amps, 2.8 meters Receptacle: BS 546	1025
-10	806-000037-000	Power cord, AC, Switzerland and Liechtenstein SEV 1011 straight, 250 volts, 10 amps, 2.8 meters Receptacle: SEV 1011	1026
-11	806-000038-000	Power cord, AC, United States (Chicago) NEMA 6-15P straight, non-locking, 250 volts, 10 amps, 1.8 meters Receptacle: NEMA 6-15R	1027

Table 6-4 Power Cord and Receptacle List (Continued)

Ref.	Part Number	Description	Feature
-12	806-000040-000	Power cord, AC, United States (Chicago) NEMA L6-15P straight, twist-lock, 250 volts, 10 amps, 1.8 meters Receptacle: NEMA L6-15R	1028
-13	806-000042-000	Power cord, AC, North America NEMA L6-15P straight, twist-lock, 250 volts, 10 amps, 2.8 meters Receptacle: NEMA L6-15R	1016
-14	806-000042-000	Power cord, AC, North America NEMA L6-15P straight, twist-lock, 250 volts, 10 amps, 2.8 meters Receptacle: NEMA L6-15R	1029
-15	806-000043-000	Power cord, AC, Japan NEMA 6-15P straight, 250 volts, 10 amps, 2.8 meters Receptacle: NEMA 6-15R	None
-16	806-000058-000	Power cord, AC, Japan JIS 8303 straight, 125 volts, 12 amps, 2.5 meters Receptacle: NEMA 5-15R	1030

This appendix lists information and error messages that appear in pop-up message boxes at the Sphereon 4500 Element Manager application.

Sphereon 4500 Element Manager Messages

This section lists Sphereon 4500 Element Manager information and error messages in alphabetical order.

A

Message	A preferred path already exists between this Source Port and this Destination Domain ID. Please reconfigure the desired path.
Description	For any source port, only one path may be defined to each destination domain ID.
Action	On the <i>Add/Change Preferred Path</i> Dialog box, change the Preferred Path.
Message	Activating this configuration will overwrite the current configuration.
Description	Confirmation message to activate a new address configuration.
Action	Click <i>Yes</i> to confirm activating the new address configuration or <i>No</i> to cancel the operation.

Message	All configuration names must be unique.
Description	All address configurations must be saved with unique names.
Action	Save the configuration with a different name that is unique to all saved configurations.
Message	All port names must be unique.
Description	A duplicate port name was entered. Every configured port name must be unique.
Action	Reconfigure the port with a unique name.
Message	Another Element Manager is currently performing a firmware install.
Description	Only one firmware install to a specific Sphereon 4500 Switch can take place at a time.
Action	Wait for the firmware install to complete and retry the operation.
Message	Are you sure you want to delete firmware version?
Description	Requesting confirmation to delete a firmware version. The firmware library can hold only eight firmware versions.
Action	Click <i>Yes</i> to confirm the firmware deletion or <i>No</i> to cancel the operation.
Message	Are you sure you want to delete this address configuration?
Description	Confirmation to delete the selected address configuration.
Action	Click <i>Yes</i> to confirm the deletion of the address configuration or <i>No</i> to cancel the operation.
Message	Are you sure you want to send firmware version?
Description	Requesting confirmation to send a firmware version.
Action	Click <i>Yes</i> to confirm the firmware send or <i>No</i> to end the operation.

C

Message	Cannot change port type while Management Style is FICON, without SANtegrity Feature. Please contact your sales representative.
Description	Firmware level is below 6.0 and user attempted to change a port type in the <i>Configure Ports</i> dialog box while FICON management style is enabled, but the optional SANtegrity Binding feature is not installed.
Action	Informational message. If the firmware is below 6.0, install SANtegrity Binding feature before changing port types in the <i>Configure Ports</i> dialog box while using FICON Management style.
Message	Cannot create partition <partition number> while FICON Management Server is enabled.
Description	The user has moved slots into a partition while the FMS server is enabled.
Action	Disable FMS before moving slots into a partition.
Message	Cannot disable switch binding while Enterprise Fabric Mode is active and the switch is online.
Description	The user attempted to disable switch binding through the <i>Switch Binding Change State</i> dialog box, but <i>Enterprise Fabric Mode</i> is enabled.
Action	Either disable <i>Enterprise Fabric Mode</i> using the <i>Enterprise Fabric Mode</i> dialog box at the SAN management application, or set the switch offline to disable switch binding.
Message	Cannot disable Insistent Domain ID while fabric binding is active.
Description	The user attempted to disable the <i>Insistent Domain ID</i> parameter through the <i>Configure Switch Parameters</i> dialog box, but fabric binding is enabled.
Action	Disable fabric binding through the <i>Fabric Binding</i> dialog box before disabling the parameter.

Message	Cannot enable beaconing on a failed FRU.
Description	Message occurs when selecting <i>Enable Beaconing</i> for a failed FRU.
Action	Replace the FRU and enable beaconing or enable beaconing on an operating FRU.
Message	Cannot enable beaconing while the system error light is on.
Description	Beaconing cannot be enabled while the system error LED is illuminated.
Action	Select <i>Clear System Error Light</i> from the <i>Products</i> menu to clear the error light, then enable beaconing.
Message	Cannot enable OpenTrunking while Enterprise Fabric Mode is active and the switch is offline.
Description	<i>Enterprise Fabric Mode</i> is active, the switch is offline, and a user is attempting to enable OpenTrunking feature. This message displays only if the feature is installed.
Action	Perform one of the following: <ul style="list-style-type: none"> • Disable <i>Enterprise Fabric Mode</i> by selecting the appropriate fabric at the fabric tree portion of the <i>Fabrics</i> view. Open the <i>Enterprise Fabric Mode</i> dialog box, click <i>Start</i>, and follow the prompts to disable the feature. • Set the director or switch online through the <i>Set Online State</i> dialog box.
Message	Cannot have E_Ports if Management Style is FICON unless SANtegrity feature is installed. Contact your sales representative.
Description	Firmware level is below 6.0 and user attempted to change Open Systems to FICON with E_ports enabled but without the SANtegrity feature installed.
Action	Informational message. If the firmware is below 6.0, if you install SANtegrity Binding feature before changing to FICON Management style, the E_Ports will remain E_Ports when you change to FICON Management style. If SANtegrity Binding feature is not installed, setting a director to FICON Management style will change all E_Ports to G_Ports.

Message	Cannot have spaces in field.
Description	Spaces are not allowed as part of the entry for this field.
Action	Delete spaces from the field entry.
Message	Cannot install firmware to a switch with a failed CTP card.
Description	Firmware cannot be installed on a switch with a failed CTP card.
Action	The CTP card failed and is not a FRU. Replace the switch.
Message	Cannot perform this operation while the switch is offline.
Description	This operation cannot be performed while the director or switch is offline.
Action	Set the director or switch offline through the <i>Set Online State</i> dialog box and retry the operation.
Message	Cannot remove all slot assignments from Partition 0.
Description	The user has attempted to remove all slots from Partition 0, which would leave the partition disabled. The director firmware requires that Partition 0 be enabled.
Action	Do not attempt to remove slots from Partition 0.
Message	Cannot retrieve current SNMP configuration.
Description	SNMP configuration information cannot be retrieved. The link is down or busy.
Action	Retry the operation later. If the condition persists, contact support personnel and report the problem.
Message	Cannot retrieve diagnostics results.
Description	Diagnostics results cannot be retrieved. The link is down or busy.

Action	Retry the operation later. If the condition persists, contact support personnel and report the problem.
Message	Cannot retrieve port configuration.
Description	The port configuration cannot be retrieved. The link is down or busy.
Action	Retry the operation later. If the condition persists, contact support personnel and report the problem.
Message	Cannot retrieve port information.
Description	Port information cannot be retrieved. The link is down or busy.
Action	Retry the operation later. If the condition persists, contact support personnel and report the problem.
Message	Cannot retrieve port statistics.
Description	Port statistics cannot be retrieved. The link is down or busy.
Action	Retry the operation later. If the condition persists, contact support personnel and report the problem.
Message	Cannot retrieve switch date and time.
Description	The switch date and time cannot be retrieved. The link is down or busy.
Action	Retry the operation later. If the condition persists, contact support personnel and report the problem.
Message	Cannot retrieve switch state.
Description	The switch state cannot be retrieved. The link is down or busy.
Action	Retry the operation later. If the condition persists, contact support personnel and report the problem.

Message	Cannot run diagnostics on a port that is failed.
Description	Port diagnostics cannot be performed on a failed port.
Action	Run diagnostics only on an operational port.
Message	Cannot run diagnostics on an active E_Port.
Description	Port diagnostics cannot be performed on a configured and active expansion port (E_Port).
Action	Run diagnostics only on an inactive E-port.
Message	Cannot run diagnostics. The port is not installed.
Description	Port diagnostics cannot be performed if the port transceiver is not installed.
Action	Install an optical transceiver or run diagnostics only on a port with an installed transceiver.
Message	Cannot save port configuration.
Description	The port configuration cannot be saved. The link is down or busy.
Action	Retry the operation later. If the condition persists, contact support personnel and report the problem.
Message	Cannot save SNMP configuration.
Description	The SNMP configuration cannot be saved. The link is down or busy.
Action	Retry the operation later. If the condition persists, contact support personnel and report the problem.
Message	Cannot set all ports to 1 Gbps due to port speed restriction on some ports.
Description	This message displays if all ports are set to 1 Gb/sec through the <i>Configure Ports</i> dialog box and some port transceivers do not support this transceiver speed.

Action	Ensure all port transceivers support 1.0625 Gigabit per second (Gbps) data transmission.
Message	Cannot set all ports to 2 Gbps due to port speed restriction on some ports.
Description	This message displays if all ports are set to 2 Gb/sec through the <i>Configure Ports</i> dialog box and some port transceivers do not support this transceiver speed.
Action	Ensure all port transceivers support 2.125 Gbps data transmission.
Message	Cannot set all ports to Negotiate due to port speed restriction on some ports.
Description	This message displays if all ports are set to <i>Negotiate</i> through the <i>Configure Ports</i> dialog box and some port transceivers do not support this configuration.
Action	Replace single-speed port transceivers with transceivers that support 1.0625 and 2.125 Gbps data transmission rates.
Message	Cannot set Fibre Channel parameters.
Description	Fibre Channel parameters cannot be set. The link is down or busy.
Action	Retry the operation later. If the condition persists, contact support personnel and report the problem.
Message	Cannot set switch date and time.
Description	The switch date and time cannot be set. The link is down or busy.
Action	Retry the operation later. If the condition persists, contact support personnel and report the problem.
Message	Cannot set switch state.
Description	The switch state cannot be set. The link is down or busy.
Action	Retry the operation later. If the condition persists, contact support personnel and report the problem.

Message	Cannot set write authorization without defining a community name.
Description	A community name was not defined in the <i>Configure SNMP</i> dialog box for the write authorization selected.
Action	Enter a community name in the name field where write authorization is checked.
Message	Cannot start data collection.
Description	Data collection cannot be started. The link is down or busy.
Action	Retry the operation later. If the condition persists, contact support personnel and report the problem.
Message	Cannot start port diagnostics.
Description	Port diagnostics cannot be started. The link is down or busy.
Action	Retry the operation later. If the condition persists, contact support personnel and report the problem.
Message	Click OK to remove all contents from log.
Description	Message requesting confirmation to delete all contents from the selected log.
Action	Click <i>OK</i> to continue or <i>Cancel</i> to end the operation.
Message	Continuing may overwrite host programming. Continue?
Description	Configurations sent from the host may be overwritten by the SAN management application.
Action	Continuing activates the current configuration and overwrites the host configuration.

Message	Could not export log to file.
Description	A log file I/O error occurred and the file could not be saved to the specified destination. The disk may be full or write protected.
Action	If the disk is full, use another disk. If the disk is write protected, change the write-protect properties or use another disk.
Message	Could not find firmware file.
Description	Firmware file selected was not found in the file transfer protocol (FTP) directory.
Action	Ensure the file name and directory are correct and retry the operation.
Message	Could not remove dump files from server.
Description	Dump files could not be removed from the server. The link may be down or the switch may be busy.
Action	Retry the operation later. If the condition persists, contact support personnel and report the problem.
Message	Could not stop port diagnostics.
Description	Port diagnostics could not be stopped. The link may be down or the switch may be busy.
Action	Retry the operation later. If the condition persists, contact support personnel and report the problem.
Message	Could not write firmware to flash.
Description	Firmware could not be written to flash memory.
Action	Retry the operation later. If the condition persists, contact support personnel and report the problem.

D

Message	Date entered is invalid.
Description	The date is entered incorrectly.
Action	Verify the number of days in the month entry is valid.
Message	Device applications should be terminated before starting diagnostics. Press NEXT to continue.
Description	A device application is not terminated.
Action	Terminate the device application before running port diagnostics.
Message	[device WWN] cannot be removed from the switch membership list while participating in switch binding. The device must be isolated from the switch, or switch binding deactivated before it can be removed.
Description	A user attempted to remove a device WWN from the switch membership list (SANTegrity binding feature) with switch binding enabled.
Action	Disconnect the device by blocking the switch port and setting the switch offline, or disable switch binding through the <i>Switch Binding Change State</i> dialog box before removing devices from the switch membership list.
Message	Disabling Insistent Domain ID will disable fabric binding. Do you want to continue?
Description	Fabric binding is enabled through the SAN management application and a user attempted to disable the <i>Insistent Domain ID</i> parameter at the <i>Configure Switch Parameters</i> dialog box.
Action	Click Yes to continue and disable fabric binding.
Message	Disabling switch binding will disable Enterprise Fabric Mode. Do you want to continue?
Description	A user attempting to disable switch binding through the <i>Switch Binding State Change</i> dialog box, but <i>Enterprise Fabric Mode</i> is enabled.

Action Disable *Enterprise Fabric Mode* at the *Enterprise Fabric Mode* dialog box before disabling switch binding.

Message **Do you want to continue with IPL?**

Description Message requesting confirmation to proceed with an IPL.

Action Click *Yes* to confirm the IPL or *Cancel* to end the operation.

Message **Duplicate community names require identical write authorizations.**

Description Duplicate community names exist that have conflicting or different write authorizations.

Action Verify community names and whether a community name is duplicated with different write authorizations.

Message **Duplicate port names detected.**

Description Ports cannot have the same name.

Action Rename ports using the *Configure Ports* option in the *Configure* menu.

E

Message **Exclusive management server connection to the director required for this command.**

Description You attempted to execute a command that is not valid when more than one management server is connected to the director.

Action Exit the additional management servers so that only one is connected to the director.

Message **Element Manager error < *number* >.**

Description The Element Manager application encountered an internal error and cannot continue.

Action Contact support personnel and report the problem.

Message	Element Manager instance is currently open.
Description	An instance of the Element Manager application is already open.
Action	Information message - no action required.
Message	Enterprise Fabric Mode will be disabled if any of the following parameters are disabled: Insistent Domain ID, Rerouting Delay, Domain RSCN's. Do you want to continue?
Description	A user attempted to disable one or more of these parameters at the <i>Configure Switch Parameters</i> dialog box with the switch online and <i>Enterprise Fabric Mode</i> (SANTegrity binding feature) enabled.
Action	Click <i>Yes</i> to continue and disable <i>Enterprise Fabric Mode</i> .
Message	Error retrieving port information.
Description	An error occurred while retrieving port information. The link is down or busy.
Action	Retry the operation. If the condition persists, contact support personnel and report the problem.
Message	Error retrieving port statistics.
Description	An error occurred while retrieving port statistics. The link is down or busy.
Action	Retry the operation. If the condition persists, contact support personnel and report the problem.
Message	Error stopping port diagnostics.
Description	An error occurred while attempting to stop the port diagnostics from running. The link is down or busy.
Action	Retry the operation. If the condition persists, contact support personnel and report the problem.

Message	Error transferring files < message >.
Description	An error occurred while transferring files from the PC hard drive to the Element Manager application. The message varies, depending on the problem.
Action	Retry the operation. If the condition persists, contact support personnel and report the problem.

F

Message	Feature not supported. The Product Name must be running version 05.00.00 or higher.
Description	The Enterprise Operating System (E/OS) version running on the switch is lower than Version 05.00.00. This message displays only if the optional OpenTrunking feature is installed.
Action	Install E/OS Version 5.00.00 or higher.

Message	Field cannot be blank.
Description	The data field requires an entry and cannot be left blank.
Action	Enter appropriate information in the data field.

Message	Field has exceeded maximum number of characters.
Description	The maximum number of characters allowed in a data entry field was exceeded.
Action	Enter information using the allowed number of characters.

Message	File transfer aborted.
Description	The user aborted the file transfer process.
Action	Verify the file transfer is to be aborted, then click <i>OK</i> to continue.

Message	File transfer is in progress.
Description	Firmware or data collection information is being transferred.
Action	Information message - no action required.

Message	Firmware download timed out.
Description	The switch did not respond in the time allowed, causing the firmware download to time out.
Action	Retry the operation. If the condition persists, contact support personnel and report the problem.
Message	Firmware file I/O error.
Description	A firmware file I/O error occurred.
Action	Retry the operation. If the condition persists, contact support personnel and report the problem.
Message	Firmware file not found.
Description	A firmware file was deleted from the management server.
Action	Add the firmware version to library.

I

Message	Incorrect product type.
Description	When configuring a new product through the <i>New Product</i> dialog box, an incorrect product was selected for the network address.
Action	Select the correct product type for the product with the network address.
Message	Installing this feature key while online will cause an IPL operation on the switch and a momentary loss of LAN connection. This operation is non-disruptive to the Fibre Channel traffic. Do you wish to continue installing this feature key?
Description	If the switch is online, installing a feature key causes a switch IPL. The LAN connection to the management server is lost momentarily, but Fibre Channel traffic is not affected.
Action	Click <i>Yes</i> to install the feature key or <i>No</i> to discontinue the operation.

Message	Internal file transfer error received from switch.
Description	The switch detected an internal file transfer error.
Action	Retry the operation. If the condition persists, contact support personnel and report the problem.
Message	Invalid character in field.
Description	An invalid character was entered in the data field.
Action	Remove invalid characters from the entry.
Message	Invalid configuration name.
Description	A user attempted to save an invalid address configuration name.
Action	Enter a configuration name of up to 24 alphanumeric characters, including spaces, hyphens and underscores.
Message	Invalid feature key.
Description	The entered feature key was not recognized.
Action	Enter the feature key again. The key is case sensitive and includes dashes.
Message	Invalid firmware file.
Description	Selected file is not a valid firmware file.
Action	Select the correct firmware file.
Message	Invalid network address.
Description	The network address specified is not known by the domain name server.
Action	Check the input address and specify the correct network address.

Message	Invalid port number. Valid ports are (0-< nn >).
Description	You have specified an invalid port number.
Action	Specify a valid port number, in the range 0 to the maximum number of ports on the product minus one. For example, for a switch with 24 ports, the valid port range is 0 to 23.
Message	Invalid response received from switch.
Description	An error occurred and the switch returned an invalid response.
Action	Resend the firmware. If the condition persists, contact support personnel and report the problem.
Message	Invalid serial number for this feature key.
Description	The switch serial number and entered feature key do not match.
Action	Ensure the entered feature key corresponds to the switch serial number.
Message	Invalid UDP port number.
Description	The user datagram protocol (UDP) port number must be an integer from 1 through 65535.
Action	Enter a port number from 1 through 65535.
Message	Invalid value for BB_Credit.
Description	The <i>BB_Credit</i> value must be an integer from 1 through 60.
Action	Enter a <i>BB_Credit</i> value from 1 through 60.
Message	Invalid value for Low BB Credit threshold (1-99) %.
Description	<i>Low BB Credit Threshold</i> text field in <i>Configure Open Trunking</i> dialog box must have entries in the range from 1 and 99. This message only displays if the optional Open Trunking feature is installed. Note that your message and the <i>Configure Open Trunking</i> dialog box may display <i>Credit Starvation Threshold</i> instead of <i>Low BB Credit Threshold</i> .

Action	Enter a value from 1 to 99 into the <i>Low BB Credit Threshold</i> of the <i>Configure Open Trunking</i> dialog box.
Message	Invalid value for day (1 - 31).
Description	The <i>Day</i> value must be an integer from 1 through 31.
Action	Enter a <i>Day</i> value from 1 through 31.
Message	Invalid value for E_D_TOV.
Description	The value for <i>E_D_TOV</i> must be an integer from 2 through 600 milliseconds.
Action	Enter an <i>E_D_TOV</i> value from 2 through 600.
Message	Invalid value for hour (0 - 23).
Description	The <i>Hour</i> value must be an integer from 0 through 23.
Action	Enter an <i>Hour</i> value from 0 through 23.
Message	Invalid value for Low BB_Credit Threshold (1 - 99%).
Description	The <i>Low BB_Credit Threshold</i> value at the <i>Configure Open Trunking</i> dialog box must be an integer from 1 through 99. This message displays only if the optional OpenTrunking feature is installed.
Action	At the <i>Configure Open Trunking</i> dialog box, enter a <i>Low BB_Credit Threshold</i> value from 1 through 99 percent.
Message	Invalid value for minute (0 - 59).
Description	The <i>Minute</i> value must be an integer from 0 through 59.
Action	Enter a <i>Minute</i> value from 0 through 59.
Message	Invalid value for month (1 - 12).
Description	The <i>Month</i> value must be an integer from 1 through 12.
Action	Enter a <i>Month</i> value from 1 through 12.

Message	Invalid value for R_A_TOV.
Description	The value for <i>R_A_TOV</i> must be an integer from 10 through 1200 milliseconds.
Action	Enter an <i>R_A_TOV</i> value from 10 through 1200 .
Message	Invalid value for second (0 - 59).
Description	The <i>Second</i> value must be an integer from 0 through 59 .
Action	Enter a <i>Second</i> value from 0 through 59 .
Message	Invalid value for Threshold (1 - 99%).
Description	The <i>Threshold %</i> value for each configured Fibre Channel port at the <i>Configure Open Trunking</i> dialog box must be an integer from 1 through 99 . This message displays only if the optional OpenTrunking feature is installed.
Action	At the <i>Configure Open Trunking</i> dialog box, enter a <i>Threshold %</i> value for each configured port from 1 through 99 percent.
Message	Invalid value for year.
Description	The <i>Year</i> value must be four digits.
Action	Enter a four-digit <i>Year</i> value.
Message	Invalid World Wide Name.
Description	The WWN format is eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx:xx:xx:xx:xx).
Action	Enter a WWN using eight two-digit hexadecimal numbers separated by colons.

L

Message	Link dropped.
Description	The switch-to-management server link was dropped.
Action	Wait approximately 30 seconds for the link to establish and retry the operation. If the condition persists, contact support personnel.
Message	Log is currently in use.
Description	The selected log is in use by another Element Manager instance.
Action	Retry the operation. If the condition persists, contact support personnel and report the problem.
Message	Loopback plug(s) must be installed on ports being diagnosed. Press NEXT to continue.
Description	An optical loopback plug must be installed in a Fibre Channel port prior to performing an external loopback diagnostic test.
Action	Ensure an optical loopback plug is installed in the port, then restart the test.

M

Message	Maximum number of versions already installed.
Description	The maximum number of firmware versions was reached.
Action	Delete a firmware version before adding a new firmware version.
Message	McDATA SANtegrity binding feature not installed. Please contact your sales representative.
Description	A user selected <i>Switch Binding</i> from the <i>Configure</i> menu. This selection is not supported because the SANtegrity binding feature is not installed.
Action	Install the optional SANtegrity binding feature key through the <i>Configure Feature Key</i> dialog box before enabling switch binding.

N

Message	Nickname already exists. Please use a different nickname.
Description	The entered nickname already exists.
Action	Specify a unique nickname.
Message	No backup configuration available to restore.
Description	A backup of the configuration is not on the management server hard drive. A configuration restore cannot be completed.
Action	Select <i>Backup and Restore Configuration</i> from the <i>Maintenance Menu</i> and select <i>Backup</i> to create a backup configuration file.
Message	No file was selected.
Description	A required file was not selected before an action was performed.
Action	Select the required file and perform the action again.
Message	No firmware version file was selected.
Description	A firmware file was not selected in the <i>Firmware Library</i> dialog box before an action was performed.
Action	Select a firmware version and perform the action again.
Message	No firmware versions to delete.
Description	There are no firmware versions in the firmware library to delete.
Action	Information message - no action required.
Message	Non-redundant switch must be offline to install firmware.
Description	Because the switch has only a single CTP card, it must be offline to initiate a firmware installation.
Action	Set switch offline and try the firmware installation again.

Message	Not all of the optical transceivers are installed for this range of ports.
Description	One or more ports in the specified port range do not have optical transceivers installed.
Action	Specify a port range valid for ports installed.

P

Message	Performing this operation will change the current state to offline.
Description	This operation causes the switch to go offline.
Action	Information message - no action required.
Message	Performing this operation will change the current state to online.
Description	This operation causes the switch to go online.
Action	Information message - no action required.
Message	Performing this action will overwrite the date/time on the switch.
Description	This warning message occurs when entering parameters through the <i>Configure Date and Time</i> dialog box, and indicates the new date and time will overwrite the existing date and time or set for the switch.
Action	Verify you intend to overwrite the switch date and time.
Message	Periodic Date/Time synchronization must be cleared before enabling switch clock alert.
Description	This action cannot be performed because the <i>Periodic Date/Time Synchronization</i> option is enabled.
Action	Click the <i>Periodic Date/Time Synchronization</i> check box at the <i>Configure Date and Time</i> dialog box to clear check mark and disable the periodic date and time synchronization option.
Message	Port binding was removed from attached devices that are also participating in switch binding.

Description	A user disabled port binding for attached devices, but one or more of the devices is controlled by fabric binding.
Action	Review the switch binding membership list to determine if devices should or should not be included.
Message	Port diagnostics cannot be performed on an inactive port.
Description	This message displays when port diagnostics are performed on an inactive port.
Action	Perform diagnostics on an active port.
Message	Port speeds cannot be configured at a higher rate than the switch speed.
Description	An attempt was made to configure a port to 2.125 Gbps with the switch speed set to 1.0625 Gbps.
Action	Set the port speed to 1.0625 Gbps at the <i>Configure Ports</i> dialog box.
Message	Preferred Paths can not be enabled until the Domain ID is set to Insistent. Disable Preferred Paths, then configure Switch Parameters.
Description	If the switch's domain ID has not been set to <i>Insistent</i> , the user is not allowed to activate the Preferred Path configuration with the <i>Enable Preferred Paths</i> check box selected.
Action	Close the <i>Configure Preferred Paths</i> dialog box and select the <i>Configure</i> menu, then <i>Operating Parameters</i> , then <i>Switch Parameters</i> . On the <i>Configure Switch Parameters</i> dialog box, select the <i>Insistent</i> check box.

R

Message	R_A_TOV must be greater than E_D_TOV.
Description	The <i>R_A_TOV</i> value must be greater than the <i>E_D_TOV</i> value.
Action	Change a value so <i>R_A_TOV</i> exceeds <i>E_D_TOV</i> .

Message	Resource is unavailable.
Description	The specified operation cannot be performed because the switch is unavailable.
Action	Verify the switch-to-management server link is operational. If the link is up, the management server may be busy. Try the operation later.

S

Message	Send firmware failed.
Description	A send firmware operation failed.
Action	Retry the operation. If the condition persists, contact support personnel and report the problem.

Message	SNMP Trap address not defined.
Description	An SNMP trap address must be defined if a community name is defined.
Action	Define an SNMP address.

Message	Stop diagnostics failed. The test is already running.
Description	Diagnostics for the port were not running and <i>Stop</i> was selected at the <i>Port Diagnostics</i> dialog box. Diagnostics aborted for some reason, but the <i>Stop</i> button remains enabled.
Action	Verify port operation. Retry diagnostics for the port and select <i>Stop</i> from the dialog box. If the condition persists, contact support personnel and report the problem.

Message	Stop diagnostics failed. The test was not running.
Description	The action to stop diagnostics failed because the test was not running.
Action	Information message - no action required.

Message	Switch binding was removed from attached devices that are also participating in port binding. Please review the port binding configuration.
----------------	----------------------------------------------------------------------------------------------------------------------------------------------------

Description	Device WWNs were removed from the switch membership list (SANtegrity binding feature), but one or more of the devices still has security controlled by port binding.
Action	Verify the security level for each device is specified as required by reviewing the <i>Bound WWN</i> list at the <i>Configure Ports</i> dialog box.
Message	System diagnostics cannot run. The operational status is invalid.
Description	System diagnostics cannot run on a switch with failed ports.
Action	Replace failed port transceivers.

T

Message	The add firmware process has been aborted.
Description	A user ended the add firmware process.
Action	Information message - no action required.
Message	The data collection process failed.
Description	An error occurred in the data collection process.
Action	Contact support personnel and report the problem.
Message	The data collection process has been aborted.
Description	A user ended the data collection process.
Action	Information message - no action required.
Message	The default zone must be disabled to configure.
Description	A user attempted to change the switch interoperability mode to <i>Open Fabric Mode</i> with the default zone enabled.
Action	Disable the default zone and repeat the operation.

Message	The management server is busy processing a request from another Element Manager.
Description	The management server could not process the current request because it is busy handling a request from another Element Manager instance.
Action	Retry the operation later. If the condition persists, contact support personnel and report the problem.
Message	The firmware file is corrupted.
Description	A firmware file contains corrupt data.
Action	Contact support personnel and report the problem.
Message	The firmware version already exists.
Description	The specified firmware version already exists in the database.
Action	Information message - no action required.
Message	The following parameters cannot be disabled while Enterprise Fabric Mode is active: Insistent Domain ID, Rerouting Delay, Domain RSCN's.
Description	A user attempted to disable one or more of these parameters at the <i>Configure Switch Parameters</i> dialog box with the switch online and <i>Enterprise Fabric Mode</i> (SANtegrity binding feature) enabled.
Action	Click <i>Yes</i> to continue and disable <i>Enterprise Fabric Mode</i> .
Message	The IPL configuration cannot be deleted.
Description	A user attempted to delete the IPL address configuration. This operation is not allowed.
Action	Cancel the operation.
Message	The link to the switch is not available.
Description	The Ethernet switch-to-management server link is not available.

Action Check the Ethernet connection. If the condition persists, contact support personnel and report the problem.

Message **The maximum number of address configurations has been reached.**

Description The maximum number of address configurations that can be saved to the management server was reached.

Action Delete configurations no longer needed to allow one or more new address configurations to be saved.

Message **The optical transceiver is not installed.**

Description Information is not available for a port without an optical transceiver installed.

Action Install an SFP optical transceiver in the port.

Message **The switch did not accept the request.**

Description The switch was not able to perform the requested action.

Action Retry the operation later. If the condition persists, contact support personnel and report the problem.

Message **The switch did not respond in the time allowed.**

Description The switch did not respond in the time allowed, causing a time out.

Action Retry the operation later. If the condition persists, contact support personnel and report the problem.

Message **The switch is busy saving maintenance information.**

Description The switch is busy performing a maintenance operation.

Action Retry the operation later. If the condition persists, contact support personnel and report the problem.

Message	The switch must be offline to configure.
Description	A configuration change was attempted that requires the switch to be set offline.
Action	Set the switch offline and retry the configuration change.
Message	This feature has not been installed. Please contact your sales representative.
Description	A user selected an option that is unavailable because a necessary feature is not installed.
Action	Contact your sales representative to obtain and install the desired optional feature.
Message	This feature key does not include all of the features currently installed and cannot be activated while the switch is online.
Description	The installed feature set contains features not being installed with the new feature key. To activate the new feature key, you must set the switch offline. Activating the new feature set removes features not in the new feature set.
Action	Set the switch offline through the <i>Set Online State</i> dialog box. Activate the new feature key using the <i>Configure Feature Key</i> dialog box.
Message	This feature key does not include all of the features currently installed. Do you want to continue with feature key activation?
Description	The installed feature set contains features not being installed with the new feature key.
Action	Click <i>Yes</i> to activate the feature key and remove current features not in the new feature set or <i>No</i> to cancel the operation.
Message	Threshold alerts are not supported on firmware earlier than 01.03.00.
Description	Threshold alerts are not supported for firmware versions released prior to Version 1.03.00.
Action	Information message - no action required.

U

Message	Unable to change incompatible firmware release.
Description	The firmware you are trying to download cannot be used for this Element Manager application release.
Action	Download compatible firmware for this Element Manager application release.
Message	Unable to save data collection file to destination.
Description	Could not save data collection file to the specified drive.
Action	Retry the operation later. If the condition persists, contact support personnel and report the problem.

Y

Message	You do not have rights to perform this action.
Description	The user does not have rights to perform the specified action.
Action	Information message - no action required.

Event Code Tables

An event is an occurrence (state change, problem detection, or problem correction) that requires user attention or that should be reported to a system administrator or service representative. An event usually indicates a switch operational state transition, but may also indicate an impending state change (threshold violation). An event may also provide information only, and not indicate an operational state change. Events are reported as event codes.

This appendix lists all three-digit event codes and provides detailed information about each code. Event codes are listed in numerical order and in tabular format, and are grouped as follows:

- 000 through 199 - system events.
- 200 through 299 - power supply events.
- 300 through 399 - fan events.
- 400 through 499 - control processor (CTP) card events.
- 500 through 599 - port events.
- 800 through 899 - thermal sensor events.

Events are recorded in the event log of the SANpilot interface, in the Spheron 4500 *Event Log* at the rack-mount management server, at a remote workstation if E-mail and call-home features are enabled, or at a simple network management protocol (SNMP) workstation. An event may also illuminate the system error (**ERR**) light-emitting diode (LED) at the switch front panel.

In addition to numerical event codes, the tables in this appendix also provide a:

- **Message** - a brief text string that describes the event.
- **Severity** - a severity level that indicates event criticality as follows:
 - 0 - informational.
 - 2 - minor.
 - 3 - major.
 - 4 - severe (not operational).
- **Explanation** - a complete explanation of what caused the event.
- **Action** - the recommended course of action (if any) to resolve the problem.
- **Event data** - supplementary event data (if any) that appears in the event log in hexadecimal format.
- **Distribution** - check marks in associated fields indicate where the event code is reported (switch, server, or attached host).

System Events (000 through 199)

Event Code: 011							
Message:	Login Server database invalid.						
Severity:	Minor.						
Explanation:	Following an initial machine load (IML) or firmware download, the Login Server database failed its cyclic redundancy check (CRC) validation. All fabric services databases initialize to an empty state, resulting in an implicit fabric logout of all attached devices.						
Action:	Perform the data collection procedure and return the CD to McDATA support personnel.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓		

Event Code: 021							
Message:	Name Server database invalid.						
Severity:	Minor.						
Explanation:	Following an IML or firmware download, the Name Server database failed its CRC validation. All fabric services databases initialize to an empty state, resulting in an implicit fabric logout of all attached devices.						
Action:	Perform the data collection procedure and return the CD to McDATA support personnel.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓		

Event Code: 031							
Message:	SNMP request received from unauthorized community.						
Severity:	Informational.						
Explanation:	An SNMP request containing an unauthorized community name was received and rejected with an error. Only requests containing authorized SNMP community names as configured through the Element Manager application are allowed.						
Action:	Add the community name to the SNMP configuration using the Element Manager application.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 051

Message:	Management Server database invalid.						
Severity:	Minor.						
Explanation:	Following an IML or firmware download, the Management Server database failed its CRC validation. All management services databases initialize to an empty state, resulting in an implicit logout of all devices logged in to the Management Server.						
Action:	Perform the data collection procedure and return the CD to McDATA support personnel.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓		

Event Code: 052							
Message:	Management Server internal error, asynchronous status report activation, or mode register update occurred.						
Severity:	Informational.						
Explanation:	An internal operating error was detected by the Management Server subsystem, an asynchronous status was reported to an attached host, or a mode register update occurred.						
Action:	<p>Management Server internal error: Perform the data collection procedure and return the CD to McDATA support personnel.</p> <p>Asynchronous status report activation: No action required.</p> <p>Mode register update: No action required.</p>						
Event Data:	<p>Supplementary data consists of reporting tasks of type eMST_SB2, with component_id eMSCID_SB2_CHPGM. For each type of error or indication, the subcomponent_id is:</p> <p>Management Server internal error: subcomponent_id is eMS_ELR_SB2_DEVICE_PROTOCOL_ERROR or eMS_ELR_SB2_MSG_PROCESSING_ERROR.</p> <p>Asynchronous status report activation: subcomponent_id is eSB2_CP_RER_ASYNC_STATUS_REPORTING.</p> <p>Mode register update: subcomponent_id is eMS_ELR_MODE_REGISTER_UPDATE.</p>						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓			✓	

Event Code: 061

Message:	Fabric Controller database invalid.						
Severity:	Minor.						
Explanation:	Following an IML or firmware download, the fabric controller database failed its CRC validation. All fabric controller databases initialize to an empty state, resulting in a momentary loss of interswitch communication.						
Action:	Perform the data collection procedure and return the CD to McDATA support personnel.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓		

Event Code: 062

Message:	Maximum interswitch hop count exceeded.						
Severity:	Informational.						
Explanation:	The fabric controller software detected that a path to another fabric element (director or switch) traverses more than seven interswitch links (ISLs or hops). This may result in Fibre Channel frames persisting in the fabric longer than standard timeout values allow.						
Action:	If possible, reconfigure the fabric so the path between any two directors or switches traverses no more than seven ISLs.						
Event Data:	Byte 0 = domain ID of the fabric element (director or switch) more than seven hops away.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 063							
Message:	Remote switch has too many ISLs.						
Severity:	Major.						
Explanation:	The fabric element (director or switch) whose domain ID is indicated in the event data has too many ISLs attached, and that element is unreachable from this switch. SAN management application Version 3.2 and earlier supports up to 32 ISLs. SAN management application Version 3.3 and later supports up to 128 ISLs.						
Action:	Reduce the ISLs on the indicated fabric element to a number within the limits specified.						
Event Data:	Byte 0 = domain ID of the fabric element (director or switch) with too many ISLs.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 070							
Message:	E_Port is segmented.						
Severity:	Informational.						
Explanation:	A switch E_Port recognized an incompatibility with the attached fabric director or switch, preventing the switch from participating in the fabric. A segmented port does not transmit Class 2 or Class 3 traffic, but transmits Class F traffic. Refer to the event data for the segmentation reason.						
Action:	Action depends on the segmentation reason specified in the event data.						
Event Data:	<p>The first byte of event data (byte 0) specifies the E_Port number. The fifth byte (byte 4) specifies the segmentation reason as follows:</p> <p>1 = Incompatible operating parameters - Either the resource allocation time out value (R_A_TOV) or error detect time out value (E_D_TOV) is inconsistent between the switch and another fabric element (director or switch). Modify the R_A_TOV and E_D_TOV to make the values consistent for all fabric elements.</p> <p>2 = Duplicate domain ID - The switch has the same preferred domain ID as another fabric element (director or switch). Modify the switch's Domain ID to make it unique.</p> <p>3 = Incompatible zoning configurations - The same name is applied to a zone for the switch and another fabric element (director or switch), but the zones contain different zone members. Modify the zone name to make it unique, or ensure zones with the same name contain identical zone members.</p> <p>4 = Build fabric protocol error - A protocol error was detected during incorporation of the switch into the fabric. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the data collection procedure and return the CD to McDATA support personnel.</p> <p>5 = No principal switch - No director or switch in the fabric can become the principal switch. Modify the switch priority to any value other than 255.</p> <p>6 = No response from attached switch (hello timeout) - The switch periodically verifies operation of attached fabric elements (directors or switches). The switch E_Port (at the operational switch) times out and segments if the attached device does not respond. Check the status of the attached director or switch. If the condition persists, perform the data collection procedure (at the attached device) and return the CD to McDATA support personnel.</p>						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 071							
Message:	Switch is isolated.						
Severity:	Informational.						
Explanation:	The switch is isolated from other fabric elements (directors or switches). This event code is accompanied by one or more 070 event codes. Refer to the event data for the segmentation reason.						
Action:	Action depends on the segmentation reason specified in the event data.						
Event Data:	<p>The first byte of event data (byte 0) specifies the E_Port number. The fifth byte (byte 4) specifies the segmentation reason as follows:</p> <p>1 = Incompatible operating parameters - Either the resource allocation time out value (R_A_TOV) or error detect time out value (E_D_TOV) is inconsistent between the switch and another fabric element (director or switch). Modify the R_A_TOV and E_D_TOV to make the values consistent for all fabric elements.</p> <p>2 = Duplicate domain ID - The switch has the same preferred domain ID as another fabric element (director or switch). Modify the switch's Domain ID to make it unique.</p> <p>3 = Incompatible zoning configurations - The same name is applied to a zone for the switch and another fabric element (director or switch), but the zones contain different zone members. Modify the zone name to make it unique, or ensure zones with the same name contain identical zone members.</p> <p>4 = Build fabric protocol error - A protocol error was detected during incorporation of the switch into the fabric. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the data collection procedure and return the CD to McDATA support personnel.</p> <p>5 = No principal switch - No director or switch in the fabric can become the principal switch. Modify the switch priority to any value other than 255.</p> <p>6 = No response from attached switch (hello timeout) - The switch periodically verifies operation of attached fabric elements (directors or switches). The switch E_Port (at the operational switch) times out and segments if the attached device does not respond. Check the status of the attached director or switch. If the condition persists, perform the data collection procedure (at the attached device) and return the CD to McDATA support personnel.</p>						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 072

Message:	E_Port connected to unsupported switch.						
Severity:	Informational.						
Explanation:	The switch is attached (through an ISL) to an incompatible fabric element (director or switch).						
Action:	Disconnect the ISL.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 073

Message:	Fabric initialization error.						
Severity:	Informational.						
Explanation:	An error was detected during the fabric initialization sequence, most likely caused by frame delivery errors. Event data is intended for engineering evaluation.						
Action:	Perform the data collection procedure and return the CD to McDATA support personnel.						
Event Data:	Byte 0 = error reason code for engineering evaluation. Bytes 4 - 9 = port numbers for which problems were detected.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 074							
Message:	ILS frame delivery error threshold exceeded.						
Severity:	Informational.						
Explanation:	Fabric controller frame delivery errors exceeded an E_Port threshold and caused fabric initialization problems (073 event code). Most fabric initialization problems are caused by control frame delivery errors, as indicated by this code. Event data is intended for engineering evaluation.						
Action:	Perform the data collection procedure and return the CD to McDATA support personnel.						
Event Data:	Byte 0 = E_Port number reporting the problem. Bytes 4 - 8 = Count of frame delivery timeouts. Bytes 9 - 11 = Count of frame delivery aborts.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 080							
Message:	Unauthorized worldwide name.						
Severity:	Informational.						
Explanation:	The WWN of the device or fabric element connected to the indicated port is not authorized for that port number.						
Action:	Change the port binding definition or connect the proper device or fabric element to the indicated port.						
Event Data:	Byte 0 = Port number reporting the unauthorized connection. Bytes 4 - 11 = WWN of the unauthorized device or fabric element.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓	✓		✓	

Event Code: 081

Message: Invalid attachment.

Severity: Informational.

Explanation: A switch port recognized an incompatibility with the attached fabric element or device and isolated the port. An isolated port does not transmit Class 2, Class 3, or Class F traffic. Refer to the event data for the reason.

Action: Action depends on the reason specified in the event data.

Event Data: The first byte of event data (byte 0) specifies the port number. The fifth byte (byte 4) specifies the isolation reason as follows:

1 = Unknown - Isolation reason is unknown, but probably caused by failure of a device attached to the switch through an **E_Port** connection. Fault isolate the failed device or contact support personnel to report the problem.

2 = ISL connection not allowed - The port connection conflicts with the configured port type. Change the port type to **F_Port** if the port is cabled to a device, or **E_Port** if the port is cabled to a fabric element to form an ISL.

3 = Incompatible switch - The switch returned a *Process ELP Reject - Unable to Process* reason code because the attached fabric element is not compatible. Set the switch operating mode to **McDATA Fabric 1.0** if connected to a McDATA product. Set the switch operating mode to **Open Fabric 1.0** if connected to an open-fabric compliant product manufactured by a different vendor.

4 = Incompatible switch - The switch returned a *Process ELP Reject - Invalid Revision Level* reason code because the attached fabric element is not compatible. Set the switch operating mode to **McDATA Fabric 1.0** if connected to a McDATA product. Set the switch operating mode to **Open Fabric 1.0** if connected to an open-fabric compliant product manufactured by a different vendor.

5 = Loopback plug connected - A loopback plug is connected to the port with no diagnostic test running. Remove the loopback plug.

6 = N_Port connection not allowed - The switch is connected to a fabric element through a port configured as an **F_port**. Change the port type to **E_Port**.

7 = Non-McDATA switch at other end - The attached fabric element is not a McDATA product. Set the switch operating mode to **Open Fabric 1.0** if connected to an open-fabric compliant product manufactured by a different vendor.

A = Unauthorized port binding WWN - The device WWN or nickname used to configure port binding for this port is not valid. At the *Configure Ports* dialog box, reconfigure the port with the WWN or nickname authorized for the attached device.

B = Unresponsive node - The attached node did not respond, resulting in a **G_Port** ELP timeout. Check the status of the attached device and clean the link's fiber-optic components (cable and connectors). If the problem persists, contact support personnel to report the problem.

Event Code: 081 (continued)							
Event Data (continued):	<p>C = ESA security mismatch - Processing of the Exchange Security Attribute (ESA) frame detected a security feature mismatch. The switch binding parameters for this switch and the attached fabric element must agree. At the <i>Switch Binding - State Change</i> dialog boxes, ensure the parameters for both fabric elements are compatible, or disable the fabric and switch binding features.</p> <p>D = Fabric binding mismatch - Fabric binding is enabled and an attached fabric element has an incompatible fabric membership list. At the <i>Fabric Binding</i> dialog box, update the fabric membership list for both fabric elements to ensure compatibility, or disable the fabric binding feature.</p> <p>E = Authorization failure reject - The fabric element connected to the switch through an ISL detected a security violation. As a result, the switch received a generic reason code and set the port to an invalid attachment state. Check the port status of the attached fabric element and clean the link's fiber-optic components (cable and connectors). If the problem persists, contact support personnel to report the problem.</p> <p>F = Unauthorized switch binding WWN - Switch binding is enabled and an attached device or fabric element has an incompatible switch membership list. At the <i>Switch Binding - Membership List</i> dialog box, update the switch membership list for the switch and the attached device or fabric element to ensure compatibility, or disable the switch binding feature.</p> <p>11 = Fabric mode mismatch - Based on the ELP revision level, a connection was not allowed because a McDATA switch in legacy mode is attached to a McDATA switch in Open Fabric mode, or a McDATA switch in Open Fabric mode is attached to an OEM switch at an incorrect ELP revision level. Update the fabric mode for one switch using the <i>Interop Mode</i> drop-down list at the <i>Configure Fabric Parameters</i> dialog box.</p> <p>12 = CNT WAN extension mode mismatch - Based on switch-to-switch differences between the ELP maximum frame sizes allowed, a connection was not allowed to a switch set to Computer Network Technologies (CNT) wide area network (WAN) extension mode. Contact McDATA support personnel to obtain software maintenance release 4.02.00. This release is required to correct the problem and allow McDATA switches to communicate with CNT UltraEdge WAN Gateways.</p>						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 120							
Message:	Error detected while processing system management command.						
Severity:	Informational.						
Explanation:	This event occurs when the switch receives a management command that violates specified boundary conditions, typically as a result of a network error. The switch rejects the command, drops the switch-to-server Ethernet link, and forces error recovery processing. When the link recovers, the command can be retried.						
Action:	No action is required for an isolated event. If this event persists, perform a data collection for this switch using the SAN management application. Save the data file to the management server CD-RW drive, and return the CD to McDATA support personnel.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 121							
Message:	Zone set activation failed - zone set too large.						
Severity:	Informational.						
Explanation:	This event occurs when the switch receives a zone set activation command that exceeds the size supported by the switch. The switch rejects the command, drops the switch-to-server Ethernet link, and forces error recovery processing. When the link recovers, the command can be modified and retried.						
Action:	Reduce the size of the zone set to conform to the limit specified, then retry the activation command.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 140							
Message:	Congestion detected on an ISL.						
Severity:	Informational.						
Explanation:	OpenTrunking firmware detected an ISL with Fibre Channel traffic that exceeded the configured congestion threshold.						
Action:	No action is required for an isolated event. If this event persists, relieve the congestion by adding parallel ISLs, increasing the ISL link speed, or moving device connections to a less-congested region of the fabric.						
Event Data:	Byte 0 = Port number reporting congestion.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 141							
Message:	Congestion relieved on an ISL.						
Severity:	Informational.						
Explanation:	OpenTrunking firmware detected an ISL with Fibre Channel traffic that previously exceeded the configured congestion threshold. The congestion is now relieved.						
Action:	No action required.						
Event Data:	Byte 0 = Port number reporting congestion relieved.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 142

Message:	Low BB_Credit detected on an ISL.						
Severity:	Informational.						
Explanation:	OpenTrunking firmware detected an ISL with no transmission BB_Credit for a period of time that exceeded the configured low BB_Credit threshold. This indicates downstream fabric congestion.						
Action:	No action is required for an isolated event or if the reporting ISL approaches 100% throughput. If this event persists, relieve the low BB_Credit condition by adding parallel ISLs, increasing the ISL link speed, or moving device connections to a less-congested region of the fabric.						
Event Data:	Byte 0 = Port number reporting low BB_Credit.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 143

Message:	Low BB_Credit relieved on an ISL.						
Severity:	Informational.						
Explanation:	OpenTrunking firmware detected an ISL with no transmission BB_Credit for a period of time that previously exceeded the configured low BB_Credit threshold. The low-credit condition is now relieved.						
Action:	No action required.						
Event Data:	Byte 0 = Port number reporting low BB_Credit relieved.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 150	
Message:	Zone merge failure.
Severity:	Informational.
Explanation:	During ISL initialization, the zone merge process failed. Either an incompatible zone set was detected or a problem occurred during delivery of a zone merge frame. This event code always precedes a 070 ISL segmentation event code, and represents the reply of an adjacent fabric element in response to a zone merge frame. Refer to the event data for the failure reason.
Action:	Action depends on the failure reason specified in the event data.
Event Data:	<p>Bytes 0 - 3 of the event data specify affected E_Port number(s). Bytes 8 - 11 specify the failure reason as follows:</p> <p>01 = Invalid data length - An invalid data length condition caused an error in a zone merge frame. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the data collection procedure and return the CD to McDATA support personnel.</p> <p>08 = Invalid zone set format - An invalid zone set format caused an error in a zone merge frame. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the data collection procedure and return the CD to McDATA support personnel.</p> <p>09 = Invalid data - Invalid data caused a zone merge failure. Inspect bytes 12 - 15 of the event data for error codes. Refer to error code definitions listed on the following page to correct the problem.</p> <p>0A = Cannot merge - A <i>Cannot Merge</i> condition caused a zone merge failure. Inspect bytes 12 - 15 of the event data for error codes. Refer to error code definitions listed on the following page to correct the problem.</p> <p>F0 = Retry limit reached - A retry limit reached condition caused an error in a zone merge frame. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the data collection procedure and return the CD to McDATA support personnel.</p> <p>F1 = Invalid response length - An invalid response length condition caused an error in a zone merge frame. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the data collection procedure and return the CD to McDATA support personnel.</p> <p>F2 = Invalid response code - An invalid response code caused an error in a zone merge frame. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the data collection procedure and return the CD to McDATA support personnel.</p>

Event Code: 150 (continued)

Event Data
(continued):

Bytes **12 - 15** of the event data specify error codes as follows:

01 = Completion fail.

03 = Zone merge error - too many zones.

04 = Zone merge error - incompatible zones.

05 = Zone merge error - too long if reason = **0A**.

06 = Zone set definition too long.

07 = Zone set name too short or not authorized.

08 = Invalid number of zones.

09 = Zone merge error - default zone states incompatible if reason = **0A**.

0A = Invalid protocol.

0B = Invalid number of zone members.

0C = Invalid flags.

0D = Invalid zone member information length.

0E = Invalid zone member information format.

0F = Invalid zone member information port.

10 = Invalid zone set name length.

11 = Invalid zone name length.

37 = Invalid zone name.

39 = Duplicate zone.

3C = Invalid number of zone members.

3D = Invalid zone member type.

3E = Invalid zone set name.

45 = Duplicate member in zone.

4A = Invalid number of zones.

4B = Invalid zone set size.

4D = Maximum number of unique zone members exceeded.

Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓				

Event Code: 151							
Message:	Fabric configuration failure.						
Severity:	Informational.						
Explanation:	A fabric-wide configuration activation process failed. An event code 151 is recorded only by the managing switch in the fabric. The event code is intended to help engineering support personnel fault isolate a fabric-wide configuration failures.						
Action:	Perform the data collection procedure and return the CD to McDATA support personnel.						
Event Data:	<p>Event data are mapped from the software implementation of the FC-SW2 protocol and are typically complicated. Decoding the event data requires engineering support. Event data are as follows:</p> <p>Bytes 0 - 3 = Managing switch domain ID in internal format (1-31). Bytes 4 - 7 = Fabric configuration operation that failed. Bytes 8 - 11 = Fabric configuration step that failed. Bytes 12 - 15 = Managed switch domain ID in internal format (1-31). Bytes 16 - 19 = Response command code received from the managed switch. Bytes 20 - 23 = Response code received from the managed switch. Bytes 24 - 27 = Reason code received from the managed switch. Bytes 28 - 31 = Error code received from the managed switch.</p>						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓				

Power Supply Events (200 through 299)

Event Code: 200							
Message:	Power supply AC voltage failure.						
Severity:	Major.						
Explanation:	AC input to the power supply is disconnected or AC circuitry in the power supply failed. The event only occurs when two power supplies are installed. The second power supply assumes the full operating load for the switch.						
Action:	Ensure the power supply is connected to facility AC power and verify operation of the facility power source. If the AC voltage does not recover (indicated by event code 203), replace the failed power supply. Perform the data collection procedure and return the CD and failed power supply to McDATA support personnel.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 201							
Message:	Power supply DC voltage failure.						
Severity:	Major.						
Explanation:	DC circuitry in the power supply failed. The event only occurs when two power supplies are installed. The second power supply assumes the full operating load for the switch.						
Action:	Replace the failed power supply. Perform the data collection procedure and return the CD and failed power supply to McDATA support personnel.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 203							
Message:	Power supply AC voltage recovery.						
Severity:	Informational.						
Explanation:	AC voltage recovered for the power supply. Both power supplies adjust to share operating load for the switch.						
Action:	No action required.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 204							
Message:	Power supply DC voltage recovery.						
Severity:	Informational.						
Explanation:	DC voltage recovered for the power supply. Both power supplies adjust to share operating load for the switch.						
Action:	No action required.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 206

Message:	Power supply removed.						
Severity:	Informational.						
Explanation:	A power supply was removed while the switch was powered on and operational. The second power supply assumes the full operating load for the switch.						
Action:	No action required or install an operational power supply.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 207

Message:	Power supply installed.						
Severity:	Informational.						
Explanation:	A redundant power supply was installed with the switch powered on and operational. Both power supplies adjust to share operating load for the switch.						
Action:	No action required.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Fan Events (300 through 399)

Event Code: 300							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	One cooling fan (out of six) failed or is rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of the power supply assembly associated with the failed fan.						
Action:	Replace the power supply assembly containing the indicated fan module.						
Event Data:	The first byte of event data (byte 0) specifies the failed fan number (0 through 5 inclusive).						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 301							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Two cooling fans (out of six) failed or are rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of the power supply assembly (or assemblies) associated with the failed fans.						
Action:	Replace the power supply assembly (or assemblies) containing the indicated fan modules.						
Event Data:	The first byte of event data (byte 0) specifies the failed fan numbers (0 through 5 inclusive).						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 302

Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Three cooling fans (out of six) failed or are rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of the power supply assembly (or assemblies) associated with the failed fans.						
Action:	Replace the power supply assembly (or assemblies) containing the indicated fan modules.						
Event Data:	The first byte of event data (byte 0) specifies the failed fan numbers (0 through 5 inclusive).						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 303

Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Four cooling fans (out of six) failed or are rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of both power supply assemblies.						
Action:	Replace both power supply assemblies.						
Event Data:	The first byte of event data (byte 0) specifies the failed fan numbers (0 through 5 inclusive).						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 304							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Five cooling fans (out of six) failed or are rotating at insufficient angular velocity. The remaining fan is operational. The amber LED illuminates at the rear of both power supply assemblies.						
Action:	Replace both power supply assemblies.						
Event Data:	The first byte of event data (byte 0) specifies the failed fan numbers (0 through 5 inclusive).						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 305							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	All six cooling fans failed or are rotating at insufficient angular velocity. The amber LED illuminates at the rear of both power supply assemblies.						
Action:	Replace both power supply assemblies.						
Event Data:	The first byte of event data (byte 0) specifies the failed fan numbers (0 through 5 inclusive).						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 310

Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	One cooling fan (out of six) recovered or the associated power supply assembly was replaced. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte 0) specifies the recovered fan number (0 through 5 inclusive).						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 311

Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Two cooling fans (out of six) recovered or the associated power supply assembly (or assemblies) were replaced. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte 0) specifies the recovered fan numbers (0 through 5 inclusive).						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 312							
Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Three cooling fans (out of six) recovered or the associated power supply assembly (or assemblies) were replaced. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte 0) specifies the recovered fan numbers (0 through 5 inclusive).						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 313							
Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Four cooling fans (out of six) recovered or both power supply assemblies were replaced. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte 0) specifies the recovered fan numbers (0 through 5 inclusive).						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 314

Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Five cooling fans (out of six) recovered or both power supply assemblies were replaced. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte 0) specifies the recovered fan numbers (0 through 5 inclusive).						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 315

Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	All six cooling fans recovered or both power supply assemblies were replaced. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte 0) specifies the recovered fan numbers (0 through 5 inclusive).						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

CTP Card Events (400 through 499)

Event Code: 400							
Message:	Power-up diagnostics failure.						
Severity:	Major.						
Explanation:	Power-on self tests (POSTs) detected a failed FRU as indicated by the event data.						
Action:	If a CTP card failure is indicated, replace the switch. If a fan or power supply failure is indicated, replace the power supply assembly. Perform the data collection procedure and return the CD and faulty FRU to McDATA support personnel.						
Event Data:	Byte 0 = FRU code as follows: 02 = CTP card, 05 = cooling fan, 06 = power supply assembly. Byte 1 = FRU slot number.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 410							
Message:	Switch reset.						
Severity:	Informational.						
Explanation:	The switch reset due to system power-up, IML, or manual reset. A software reset can occur automatically after a firmware fault (event code 411), or be user-initiated. Event data indicates the type of reset.						
Action:	No action required.						
Event Data:	Byte 0 = reset type as follows: 00 = power-on, 02 = IML, 04 = reset.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 411

Message:	Firmware fault.						
Severity:	Major.						
Explanation:	Switch firmware encountered an unexpected condition and dumped operating state information to FLASH memory for retrieval and analysis. The dump file automatically transfers from the switch to the management server, where it is stored for later retrieval through the data collection procedure. The switch performs a software reset, during which all attached Fibre Channel devices are momentarily disrupted, log out, and log back in.						
Action:	Perform the data collection procedure and return the CD to McDATA support personnel.						
Event Data:	Bytes 0 - 3 = fault identifier, least significant byte first.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 412

Message:	CTP watchdog timer reset.						
Severity:	Informational.						
Explanation:	The hardware watchdog timer expired and caused the CTP card to reset.						
Action:	Perform the data collection procedure and return the CD to McDATA support personnel.						
Event Data:	Byte 0 = reset type as follows: 00 = task switch did not occur within approximately one second, 01 = interrupt servicing blocked for more than approximately one second.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 421							
Message:	Firmware download complete.						
Severity:	Informational.						
Explanation:	A new firmware version was downloaded to the switch from the management server or SANpilot interface. Event data contains the ASCII firmware version in hexadecimal format xx.yy.zz.bbbb .						
Action:	No action required.						
Event Data:	Bytes 0 and 1 = release level (xx). Bytes 6 and 7 = interim release level (zz). Byte 2 = always a period. Byte 8 = always a space. Bytes 3 and 4 = maintenance level (yy). Bytes 9 - 12 = build ID (bbbb). Byte 5 = always a period.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 423							
Message:	CTP firmware download initiated.						
Severity:	Informational.						
Explanation:	The management server or SANpilot interface initiated download of a new firmware version to the switch.						
Action:	No action required.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 426

Message:	Multiple ECC single-bit errors occurred.						
Severity:	Minor.						
Explanation:	When the SDRAM controller detects an error checking and correction (ECC) error, an interrupt occurs. If an interrupt occurs a certain number of times weekly, a 426 event code is recorded. The number of interrupts is indicated by the event data.						
Action:	No action required. SDRAM is probably malfunctioning intermittently.						
Event Data:	Byte 0 of the event data (equal to 5 , 10 , 15 , or 20) is recorded. The number of interrupts equals two to the power of the event data. Event data equal to 10 indicates 1,024 ECC error interrupts.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 433

Message:	Nonrecoverable Ethernet fault.						
Severity:	Major.						
Explanation:	A non-recoverable Ethernet interface failure was detected and the LAN connection to the management server or Internet was terminated. No failure information or event codes are reported outside the switch. Although Fibre Channel port functionality is not affected, the switch cannot be monitored or configured.						
Action:	Replace the switch.						
Event Data:	Byte 0 = LAN error type as follows: 01 = hard failure, 04 = registered fault. Byte 1 = LAN error subtype (internally defined). Byte 2 = LAN fault identifier (internally defined).						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 440							
Message:	Embedded port hardware failed.						
Severity:	Major.						
Explanation:	The embedded port hardware detected a fatal error.						
Action:	Replace the switch.						
Event Data:	Byte 0 = CTP slot position (00). Byte 1 = engineering reason code Bytes 4 - 7 = elapsed millisecond tick count.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 442							
Message:	Embedded port anomaly detected.						
Severity:	Informational.						
Explanation:	The switch detected a deviation in the normal operating mode or status of the embedded port.						
Action:	No action required. An additional event code is generated if this incident exceeds an error threshold or results in a port failure.						
Event Data:	Byte 0 = embedded port number. Byte 1 = anomaly reason code. Bytes 4 - 7 = elapsed millisecond tick count. Bytes 8 and 9 = high-availability error callout #1. Bytes 10 and 11 = high-availability error callout #2. Byte 12 = detecting port. Byte 13 = connected port. Bytes 16 and 17 = high-availability error callout #3. Bytes 18 and 19 = high-availability error callout #4.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 445							
Message:	ASIC detected a system anomaly.						
Severity:	Informational.						
Explanation:	The application-specific integrated chip (ASIC) detected a deviation in the normal operating mode or operating status of the switch.						
Action:	No action required. An additional event code is generated if this incident exceeds an error threshold that results in a system event.						
Event Data:	Byte 0 = embedded port number. Byte 1 = anomaly reason code. Bytes 4 - 7 = elapsed millisecond tick count. Bytes 8 and 9 = high-availability error callout #1. Bytes 10 and 11 = high-availability error callout #2. Byte 12 = detecting port. Byte 13 = connected port. Bytes 16 and 17 = high-availability error callout #3. Bytes 18 and 19 = high-availability error callout #4.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 453							
Message:	New feature key installed.						
Severity:	Informational.						
Explanation:	This event occurs when a new feature key is installed from the management server or SANpilot interface. The switch performs an IPL when the feature key is enabled. Event data indicates which feature(s) are installed.						
Action:	No action required.						
Event Data:	Byte 0 = feature description as follows: 00 - 04 = Flexport Technology, 06 = Open-system management server. Byte 1 = feature description as follows: 06 = SANtegrity binding, 07 = OpenTrunking.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Port Events (500 through 599)

Event Code: 506							
Message:	Fibre Channel port failure.						
Severity:	Major.						
Explanation:	A Fibre channel port failed. The amber LED corresponding to the port illuminates to indicate the failure. Other ports remain operational if their LEDs are extinguished.						
Action:	Perform the data collection procedure and return the CD to McDATA support personnel. Perform a switch reset. If the problem persists, replace the switch.						
Event Data:	Byte 0 = port number (00 - 23). Byte 1 = engineering reason code. Bytes 4 - 7 = elapsed millisecond tick count. Bytes 8 - 11 = reason code specific. Byte 16 = connector type. Bytes 17 and 18 = transmitter technology. Byte 19 = distance capabilities. Byte 20 = supported transmission media. Byte 21 and 22 = speed capability and configuration.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 507							
Message:	Loopback diagnostics port failure.						
Severity:	Informational.						
Explanation:	A loopback diagnostic test detected a Fibre Channel port failure.						
Action:	No action required. An event code 506 is generated if this diagnostic failure results in a hard port failure.						
Event Data:	Byte 0 = port number (00 - 23). Byte 1 = engineering reason code. Bytes 4 - 7 = elapsed millisecond tick count. Bytes 8 - 11 = reason code specific. Byte 12 = test type.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 508							
Message:	Fibre Channel port anomaly detected.						
Severity:	Informational.						
Explanation:	The switch detected a deviation in the normal operating mode or status of the indicated Fibre Channel port.						
Action:	No action required. An event code 506 is generated if this anomaly results in a hard port failure.						
Event Data:	Byte 0 = port number (00 - 23). Byte 1 = anomaly reason code. Bytes 4 - 7 = elapsed millisecond tick count. Bytes 8 and 9 = high-availability error callout #1. Bytes 10 and 11 = high-availability error callout #2. Byte 12 = detecting port. Byte 13 = connected port. Bytes 16 and 17 = high-availability error callout #3. Bytes 18 and 19 = high-availability error callout #4.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 510							
Message:	SFP optical transceiver hot-insertion initiated.						
Severity:	Informational.						
Explanation:	Installation of an SFP optical transceiver was initiated with the switch powered on and operational. The event indicates operational firmware detected the presence of the transceiver.						
Action:	No action required.						
Event Data:	Byte 0 = port number (00 - 23) Bytes 4 - 7 = elapsed millisecond tick count.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 512							
Message:	SFP optical transceiver nonfatal error.						
Severity:	Minor.						
Explanation:	Switch firmware detected an SFP optical transceiver non-fatal error.						
Action:	Replace the failed transceiver with a functional transceiver of the same type.						
Event Data:	Byte 0 = port number (00 - 23). Byte 1 = engineering reason code. Bytes 4 - 7 = elapsed millisecond tick count.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 513							
Message:	SFP optical transceiver hot-removal completed.						
Severity:	Informational.						
Explanation:	An SFP optical transceiver was removed while the switch was powered on and operational.						
Action:	No action required.						
Event Data:	Byte 0 = port number (00 - 23) Bytes 4 - 7 = elapsed millisecond tick count.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 514

Message:	SFP optical transceiver failure.						
Severity:	Major.						
Explanation:	An SFP optical transceiver failed. The amber LED corresponding to the port illuminates to indicate the failure. Other ports remain operational if their LEDs are extinguished.						
Action:	Replace the failed transceiver with a functional transceiver of the same type.						
Event Data:	Byte 0 = port number (00 - 23). Byte 1 = engineering reason code. Bytes 4 - 7 = elapsed millisecond tick count.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 523

Message:	FL_Port open request failed.						
Severity:	Informational.						
Explanation:	When the indicated FL_Port attempted to open a loop device, the port open (OPN) sequence was returned.						
Action:	No action required.						
Event Data:	Byte 0 = port number (00 - 23). Byte 1 = arbitrated loop physical address (AL_PA) of the device transmitting the OPN sequence.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 524							
Message:	No AL_PA acquired.						
Severity:	Informational.						
Explanation:	Switch cannot allocate an AL_PA of 0 (loop master) for an FC-AL device during loop initialization. The device cannot participate in loop operation.						
Action:	Disconnect the FC-AL device that is loop master.						
Event Data:	Byte 0 = port number (00 - 23).						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 525							
Message:	FL_Port arbitration timeout.						
Severity:	Informational.						
Explanation:	A switch port could not win loop arbitration within the specified loop protocol time out value (LP_TOV).						
Action:	Switch firmware reinitializes the arbitrated loop. No user action required.						
Event Data:	Byte 0 = port number (00 - 23).						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 581

Message:	Implicit incident.						
Severity:	Major.						
Explanation:	An attached open systems interconnection (OSI) server recognized a condition caused by an event that occurred at the server. The event caused an implicit Fibre Channel link incident.						
Action:	A link incident record (LIR) is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to MAP 0000: Start MAP on page 3-6 to perform fault isolation.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
							✓

Event Code: 582

Message:	Bit error threshold exceeded.						
Severity:	Major.						
Explanation:	An attached OSI server determined the number of code violation errors recognized exceeded the bit error threshold.						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to MAP 0000: Start MAP on page 3-6 to perform fault isolation.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
							✓

Event Code: 583							
Message:	Loss of signal or loss of synchronization.						
Severity:	Major.						
Explanation:	An attached OSI server recognized a loss-of-signal condition or a loss-of-synchronization condition that persisted for more than the specified receiver-transmitter timeout value (R_T_TOV).						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to MAP 0000: Start MAP on page 3-6 to perform fault isolation.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
							✓

Event Code: 584							
Message:	Not operational primitive sequence received.						
Severity:	Major.						
Explanation:	An attached OSI server received a not-operational primitive sequence (NOS).						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to MAP 0000: Start MAP on page 3-6 to perform fault isolation.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
							✓

Event Code: 585

Message:	Primitive sequence timeout.						
Severity:	Major.						
Explanation:	An attached OSI server recognized either a link reset (LR) protocol timeout or a timeout while waiting for the appropriate response (while in a NOS receive state and after NOS was not longer recognized).						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to MAP 0000: Start MAP on page 3-6 to perform fault isolation.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
							✓

Event Code: 586

Message:	Invalid primitive sequence received for current link state.						
Severity:	Major.						
Explanation:	An attached OSI server recognized either a link reset (LR) or a link-reset response (LRR) sequence while in the wait-for-online sequence (OLS) state.						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to MAP 0000: Start MAP on page 3-6 to perform fault isolation.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
							✓

Thermal Sensor Events (800 through 899)

Event Code: 810							
Message:	High temperature warning (CTP card thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with the CTP2 card indicates the warm temperature threshold was reached or exceeded.						
Action:	Perform the data collection procedure and return the CD to McDATA support personnel. Perform a switch reset. If the problem persists, replace the switch.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 811							
Message:	Critically hot temperature warning (CTP card thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with the CTP2 card indicates the hot temperature threshold was reached or exceeded.						
Action:	Perform the data collection procedure and return the CD to McDATA support personnel. Perform a switch reset. If the problem persists, replace the switch.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Restore Management Server

The procedure in this appendix provides information to restore the rack-mount management server after a failure of the server hard drive. The procedure includes restoration of the:

- Windows 2000 Professional operating system.
- Windows 2000 configuration information.
- Storage area network (SAN) management application (SANavigator 4.0 or EFCM 8.0) and Sphereon 4500 Element Manager application.
- SAN management data directory.

Requirements

The following are required to perform this procedure:

- **Management Server Restore CD-ROM** - This CD-ROM is shipped with the management server and contains the:
 - Disk operating system (DOS) files required to boot the PC after a hard drive failure.
 - Windows 2000 Professional operating system.
- **EFC Management Applications CD-ROM** - This CD-ROM contains the SAN management application (SANavigator 4.0 or EFCM 8.0) and Sphereon 4500 Element Manager application.

- **SAN Management data directory backup on CD-ROM** - The SAN management data directory is automatically backed up to a CD when the management server is rebooted or when the data directory contents change. The data directory includes:
 - All configuration data (product definitions, user names, passwords, user rights, nicknames, session options, simple network management protocol (SNMP) trap recipients, E-mail recipients, and Ethernet event notifications).
 - All log files (SAN management application logs and individual Element Manager logs).
 - Zoning library (all zone set and zone definitions).
 - Firmware library.
 - Call-home settings.
 - Configuration data for each managed Sphereon 4500 Switch (stored on the management server and in NV-RAM on each switch).
- **Windows 2000 configuration information** - Windows 2000 network addresses, date and time information, user information, and the product identification are recorded during installation of the management server. Refer to [Task 14: Record or Verify Server Restore Information](#) on page 2-78 for information.

Restore Management Server Procedure

To restore the rack-mount management server:

1. At the management server, press the left edge (**PUSH** label) of the LCD panel to disengage the panel and expose the CD-RW drive.
2. Insert the *Management Server Restore* CD-ROM in the CD-RW drive and close the LCD panel.

ATTENTION ! This procedure deletes all data from the C: hard drive partition.

3. Press the power () button. The server powers on and performs the restore process from the CD-ROM.

4. After the restore process completes, the server makes an audible series of beeps. Remove the *Management Server Restore* CD-ROM from the CD-RW drive.
5. Power cycle the management server. The server performs power-on self-tests (POSTs). After successful POST completion, the LCD panel displays a **Welcome!!** message, then continuously cycles through and displays server operational information.
6. Configure the following parameters at the server's LCD panel. Refer to [Task 7: Configure Server Password and Network Addresses](#) on page 2-51 for instructions.
 - LCD panel password.
 - IP address for private and public LAN connections.
 - Subnet mask for private and public LAN connections.
7. Log on to the server's Windows 2000 desktop through a LAN connection to a browser-capable PC. Refer to [Access the Management Server Desktop](#) on page 2-55 for instructions.
8. Configure Windows 2000 configuration information as required by the customer:
 - Configure computer and workgroup names for the management server. If required, change the server's gateway address and DNS server IP address to conform to the customer's LAN addressing scheme. Refer to [Task 8: Configure Management Server Information](#) on page 2-55 for instructions.
 - Change the default Windows 2000 administrator password and configure password access for authorized users. Refer to [Task 9: Configure Windows 2000 Users](#) on page 2-63 for instructions.
 - Set the server's date and time. Refer to [Task 10: Set Management Server Date and Time](#) on page 2-69 for instructions.
 - Configure the call-home feature. Refer to [Task 11: Configure the Call-Home Feature \(Optional\)](#) on page 2-71 for instructions.
9. Insert the *EFC Management Applications* CD-ROM in the CD-RW drive and close the LCD panel.
10. At the management server's Windows 2000 desktop, click *Start* at the left side of the task bar, then select the *Run* option. The *Run* dialog box displays ([Figure C-1](#) on page C-4).

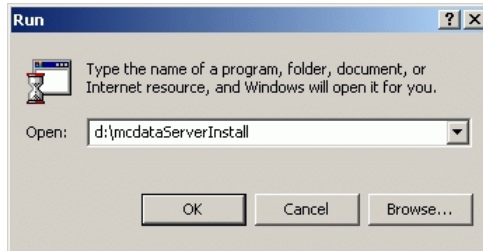


Figure C-1 Run Dialog Box

11. At the *Run* dialog box, type **D:\mcdataServerInstall** in the *Open* field.
12. Click **OK**. A series of message boxes appear as the *InstallAnywhere* third-party application prepares to install the SAN management software, followed by the *McDATA EFC Management Applications* dialog box.
13. Follow the online instructions for the *InstallAnywhere* program. Click *Next*, *Install*, or *Done* as appropriate.
14. Remove the *EFC Management Applications* CD-ROM from the CD-RW drive.
15. Insert the SAN management data directory backup CD-ROM (created while performing [Task 20: Back Up Configuration Data](#) on page 2-115) in the CD-RW drive and close the LCD panel.
16. Copy the contents of the CD-ROM to the management server's hard drive as follows:
 - For the Sanavigator 4.0 application, copy the CD-ROM contents to the following directories:
 - **C:\Program Files\SANavigator4.0\CallHome**
 - **C:\Program Files\SANavigator4.0\Client**
 - **C:\Program Files\SANavigator4.0\Server.**
 - For the EFCM 8.0 application, copy the CD-ROM contents to the following directories:
 - **C:\Program Files\EFCM 8.0\CallHome**
 - **C:\Program Files\EFCM 8.0\Client**
 - **C:\Program Files\EFCM 8.0\Server.**

17. Power off and reboot the management server.
 - a. At the Windows 2000 desktop, click *Start* at the left side of the task bar (bottom of the desktop), then select *Shut Down*. The *Shut Down Windows* dialog box displays.
 - b. Select the *Restart* option from the list box and click *OK*. The server powers down and restarts. During the reboot process the LAN connection between the server and browser-capable PC drops momentarily, and the TightVNC viewer displays a network error.
 - c. After the server reboots, click *Login again*. The *VNC Authentication* screen displays (Figure C-2).

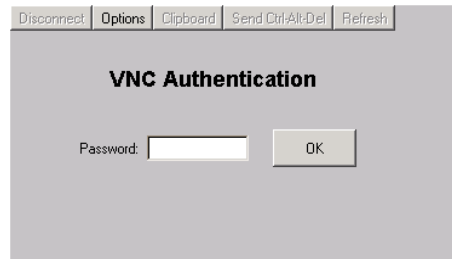


Figure C-2 VNC Authentication Screen

- d. Type the default password and click *OK*. The *Welcome to Windows* dialog box displays (Figure C-3).

NOTE: The default TightVNC viewer password is **password**.

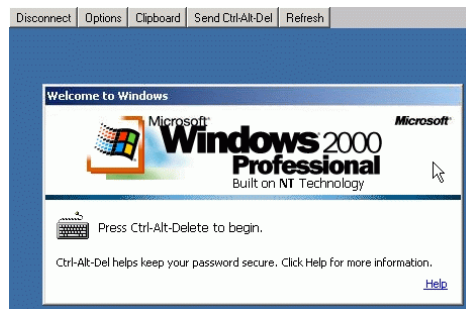


Figure C-3 Welcome to Windows Dialog Box

- e. Click the **Send Ctrl-Alt-Del** button at the top of the window to log on to the management server desktop. The *Log On to Windows* dialog box displays (Figure C-4).

NOTE: Do not simultaneously press the **Ctrl**, **Alt**, and **Delete** keys. This action logs the user on to the browser-capable PC, not the rack-mount management server.



Figure C-4 Log On to Windows Dialog Box

- f. Type the default Windows 2000 user name and password and click **OK**. The server's Windows 2000 desktop opens and the *SANavigator Log In* or *EFCM Log In* dialog box displays (Figure C-5 on page C-7).

NOTE: The default Windows 2000 user name is **Administrator** and the default password is **password**. The user name and password are case-sensitive.



Figure C-5 SANavigator Log In or EFCM Log In Dialog Box

- g. Type the SAN management application default user ID and password and select a server or IP address from the *Network Address* drop-down list.

NOTE: The default SAN management application user name is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

- h. Click *Login*. The application opens and the SANavigator or EFCM main window appears.

Consolidating Management Servers

This appendix provides instructions to consolidate multiple rack-mount management servers by configuring one unit as the server and configuring the remaining units as clients backups. The appendix provides the following sections:

- Overview.
- Consolidating management servers.
- Reconfiguring a client after an management server failure.

Overview

For control and efficiency, directors and switches in a multiswitch fabric should be managed by a single management server. When multiple servers communicate with directors and switches, the control environment should be consolidated to one rack-mount server. The remaining servers should be configured as client backups.

Although there can be multiple server configurations, the two configurations described as follows are the most probable and are addressed in this appendix.

- Multiple management servers ([Figure D-1](#) on page D-2), each with one Ethernet media adapter connected to a private network (LAN 2) that provides director and switch attachment. The second Ethernet media adapter (LAN 1) is not connected.

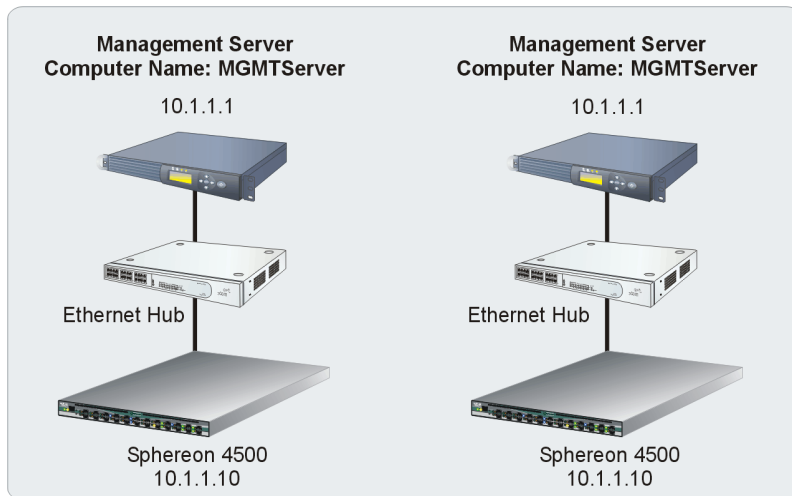


Figure D-1 Servers Before Consolidation (Private LAN Connection Only)

- Multiple management servers (Figure D-2), each with one Ethernet media adapter connected to the private director and switch network (LAN 2), and a second Ethernet media adapter connected to the customer's corporate intranet (LAN 1).

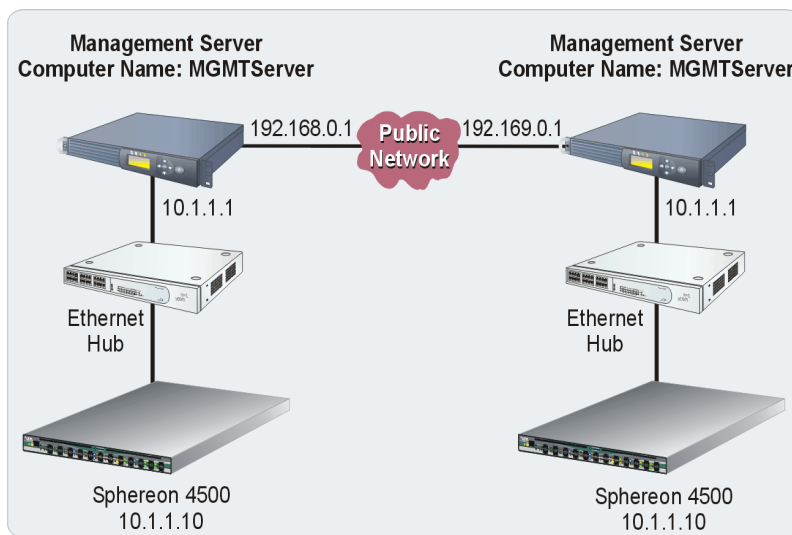


Figure D-2 Servers Before Consolidation (Private and Public LAN Connections)

Required SAN Management Application Version

Before consolidating management servers, ensure each rack-mount server is running Version 4.0 (or later) of the SANavigator application or Version 8.0 (or later) of the EFCM application, and each switch is running firmware Version 6.0 (or later). If the SAN management application requires upgrade, refer to [Install or Upgrade Software](#) on page 4-87 for instructions. If the switch firmware requires upgrade, refer to [Manage Firmware Versions](#) on page 4-59 for instructions.

IP Address Assignment

All Sphereon 4500 Switches (or other McDATA managed products) and all management servers participating in a multiswitch fabric must have unique Internet Protocol (IP) addresses. McDATA directors, switches, and servers are shipped with the following default IP addresses:

- Directors and switches: **10.1.1.10**.
- Rack-mount management server:
 - Private (LAN 2) Ethernet adapter: **10.1.1.1**.
 - Public (LAN 1) Ethernet adapter: **192.168.0.1**.

[Figure D-3](#) shows typical IP address assignments (without leading zeros) in a multiswitch environment.

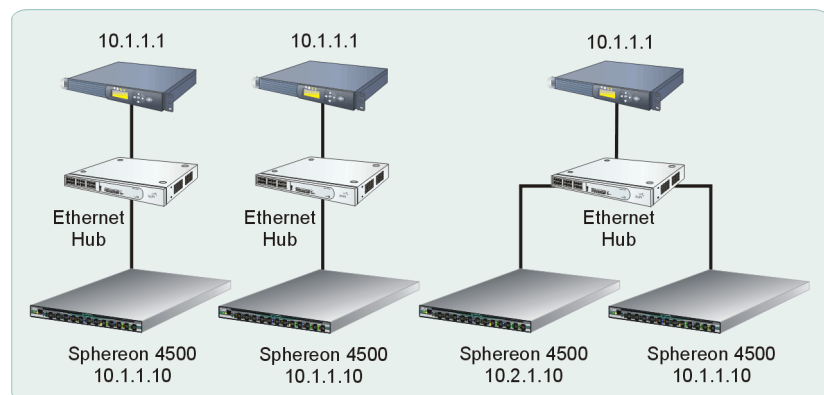


Figure D-3 IP Addresses in a Multiswitch Environment (Before Consolidation)

IP addresses are structured to represent a location and product type. The address format is **010.rrr.ppp.xxx**, where:

- **rrr** is the cabinet number (**001**, **002**, or **003**), which specifies the location of a stand-alone product or McDATA FC-512 Fabriccenter equipment cabinet. The numbers have no hierarchical significance and do not have to reflect physical order along a LAN. However, you must assign a different number to each stand-alone product or cabinet.

NOTE: Procedures in this appendix assume the cabinet at location 1 (**001**) is associated with the management server, and cabinets connected to client servers are numbered in the physical order shown in [Figure D-3](#).

- **ppp** is the product type as follows:
 - **001** for a rack-mount management server.
 - **003** for an ES-1000 Switch.
 - **005** for an ED-5000 Director.
 - **006** for an ES-3016 Switch.
 - **007** for an ES-3032 Switch.
 - **008** for an Intrepid 6064 Director.
 - **009** for a Sphereon 3216 Switch.
 - **010** for a Sphereon 3232 Switch.
 - **011** for an Intrepid 6140 Director.
 - **012** for a Sphereon 4500 Switch.
- **xxx** is the physical position (top to bottom) of the server, director, or switch in a Fabriccenter equipment cabinet as follows:
 - **001** for a rack-mount management server.
 - **001** for the lowest director or switch of the first model, **002** for the next director or switch of the same model.
 - **001** for the lowest director or switch of the second model, **002** for the next director or switch of the same model.

NOTE: Use position number **001** for stand-alone directors or switches.

Consolidating Management Servers

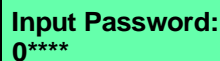
This procedure provides instructions to consolidate multiple management servers into a single environment. The procedure is divided into steps that are:

- Common for all configurations.
- Unique to the private LAN configuration.
- Unique to the public LAN and corporate intranet configuration.

Common Steps for All Configurations

Perform the following steps for the switch configurations shown in [Figure D-1](#) on page D-2 and [Figure D-2](#) on page D-2:

1. Designate one rack-mount server as the management server (as directed by the customer's network administrator) and the remaining servers as client backups.
2. Ensure each rack-mount server has a unique IP address configured for the *right* RJ-45 adapter (LAN 2) at the rear of the server. Repeat this step for the management server and all client servers.
 - a. At the server's LCD panel, press **ENTER**. The **Welcome!!** or operational information message changes to the following ([Figure D-4](#)):



Input Password:
0****

Figure D-4 LCD Panel (Password Entry)

- b. Using the ▲ button to increment a digit, the ▼ button to decrement a digit, the ◀ button to move the cursor left, and the ▶ button to move the cursor right, input the default or changed password, and press **ENTER**. The **LAN 1 Setting??** message appears at the LCD panel.
- c. Press the ▼ button. The **LAN 2 Setting??** message appears at the LCD panel. Press **ENTER** and the following message appears ([Figure D-5](#) on page D-6) with the default IP address of 10.1.1.1.

A green rectangular box with a black border containing the text "Input IP:" followed by "010.001.001.001" on the next line.

Figure D-5 LCD Panel (LAN 2 IP Address)

- d. Use the arrow keys as described in [step b](#) to input a unique IP address for each rack-mount server. For example:
- Management server: **10.1.1.1**
 - First client backup server: **10.2.1.1**
 - Second client backup server: **10.3.1.1**
 - Third client backup server: **10.4.1.1**
- e. Press **ENTER**. The following message appears ([Figure D-6](#)):

A green rectangular box with a black border containing the text "Save Change?" followed by "Yes, Save !!" on the next line.

Figure D-6 LCD Panel (Save Change)

- f. Press **ENTER**. The LAN 2 IP address changes and the following message appears ([Figure D-7](#)) with the default subnet mask of **255.0.0.0**.

A green rectangular box with a black border containing the text "Input Netmask:" followed by "255.000.000.000" on the next line.

Figure D-7 LCD Panel (LAN 2 Subnet Mask)

- g. Use the arrow keys as described in [step b](#) to input a new subnet mask (if required by the customer's network administrator), then press **ENTER**. The following message appears ([Figure D-8](#)):

A green rectangular box with a black border containing the text "Save Change?" followed by "Yes, Save !!" on the next line.

Figure D-8 LCD Panel (Save Change)

- h. Press **ENTER**. A **Wait a moment!** message appears at the LCD panel, the LCD panel returns to the **LAN 1 Setting??** message, and the LAN 2 subnet mask changes.
3. Ensure each server has a unique computer name. Repeat this step for the management server and all client servers.
 - a. Log on to the server's Windows 2000 desktop through a LAN connection to a browser-capable PC. Refer to [Access the Management Server Desktop](#) on page 2-55 for instructions.
 - b. At the Windows 2000 desktop, click *Start* at the left side of the task bar (bottom of the desktop), then select *Settings*, then *Control Panel*. The *Control Panel* window displays.
 - c. Double-click the *System* icon. The *System Properties* dialog box displays with the *General* tab selected as the default.
 - d. Click the *Network Identification* tab. The *System Properties* dialog box displays with the *Network Identification* tab selected ([Figure D-9](#)).

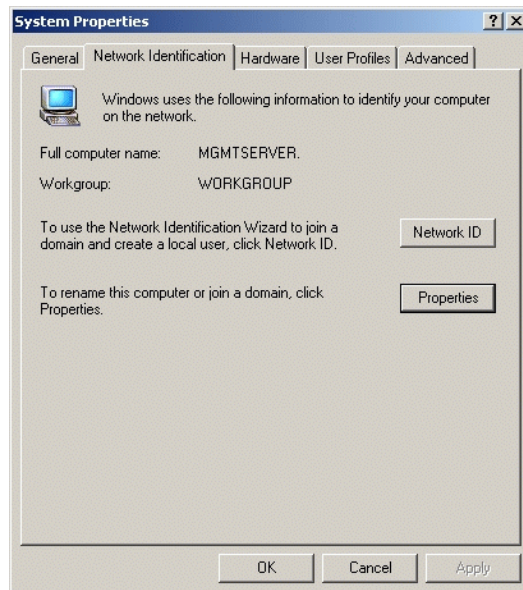


Figure D-9 System Properties Dialog Box (Network Identification Tab)

- e. Click *Properties*. The *Identification Changes* dialog box displays (Figure D-10).

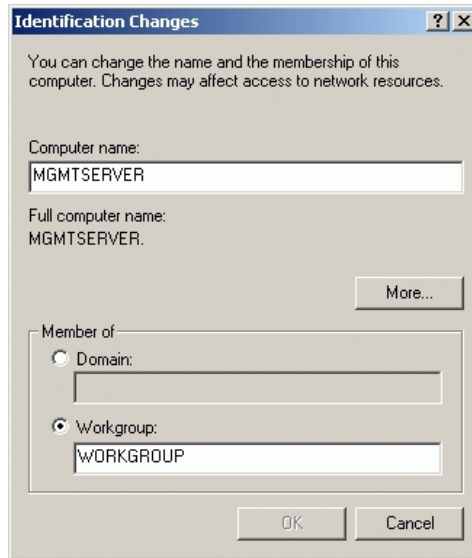


Figure D-10 Identification Changes Dialog Box

- f. At the *Computer Name* field, input a unique name for each rack-mount server. For example:
- Management server: **MGMTSERVER**
 - First client backup server: **CLIENT1**
 - Second client backup server: **CLIENT2**
 - Third client backup server: **CLIENT3**
- g. For each server, change the workgroup name to **WORKGROUP**, then click *OK*. The dialog box closes.
- h. At the *System Properties* dialog box, click *OK* to close the dialog box and return to the *Control Panel* window.
- i. Click close (X) at the upper right corner of the *Control Panel* window to return to the Windows 2000 desktop.

4. Ensure each Sphereon 4500 Switch has a unique IP address.
 - a. Change the IP address of a switch through the maintenance port at the rear of the switch chassis ([Task 5: Configure Switch Network Information \(Optional\)](#) on page 2-41).
 - b. If the IP address is changed at a switch, the IP address must also be changed at the SAN management application (management server) ([Task 13: Configure the Switch to the Management Application](#) on page 2-76).

After performing the preceding steps, [Figure D-11](#) shows unique IP addresses for all servers and switches.

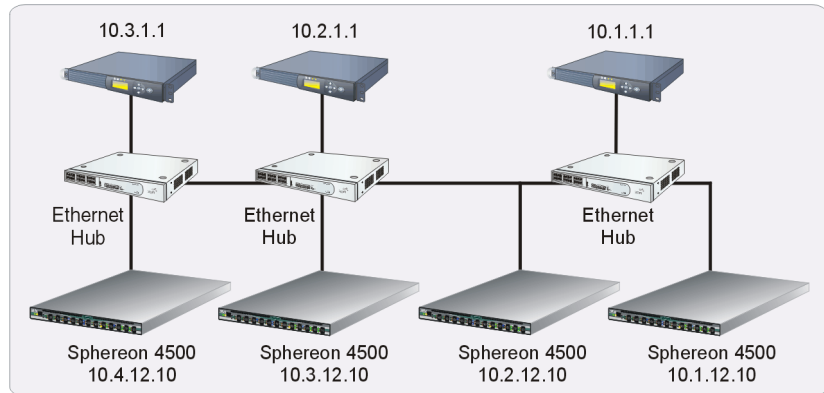


Figure D-11 IP Addresses in a Multiswitch Environment (After Consolidation)

5. Define all switches formerly managed by client backup PCs to the management server. Repeat this step for all switches defined to the management server.
 - a. At the SAN management application (SANavigator or EFCM main window), select the *Setup* option from the *Discover* menu. The *Discover Setup* dialog box displays ([Figure D-12](#) on page D-10).

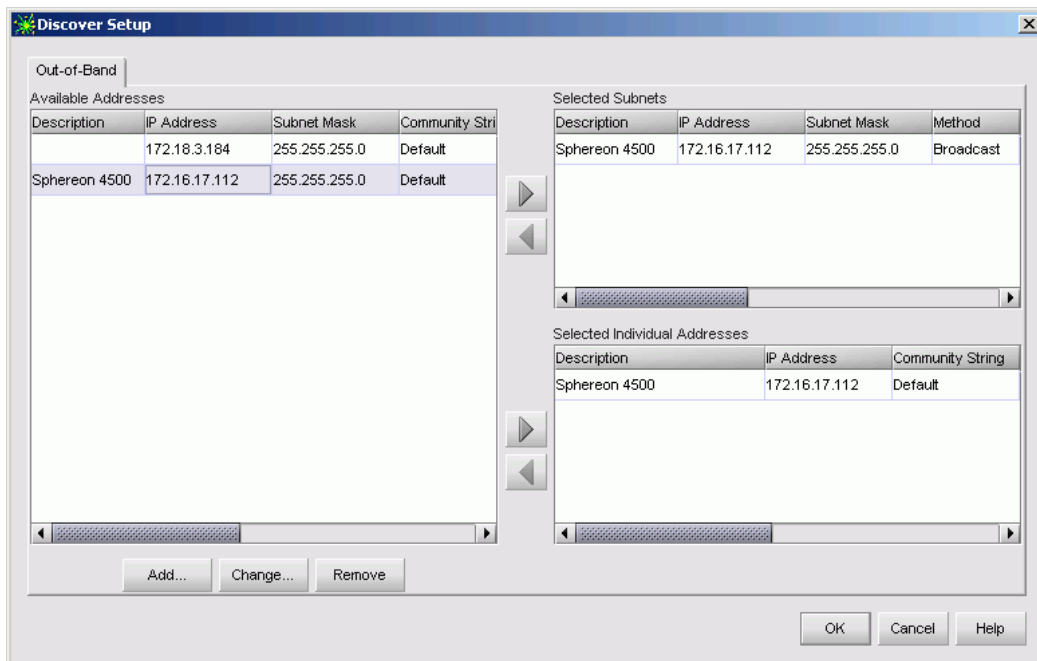


Figure D-12 Discover Setup Dialog Box

- b. Click *Add*. The *Domain Information* dialog box displays with the *IP Address* page open by default (Figure D-13 on page D-11).
- c. Type a switch description (**Sphereon 4500**, for example) in the *Description* field.
- d. Type the switch IP address (determined by the customer's network administrator) in the *IP Address* field.
- e. Type the switch subnet mask (determined by the customer's network administrator) in the *Subnet Mask* field.
- f. At the *Data Source for Domain* area of the dialog box, select the *Use auto detection*, *Use the server*, or *Use a specific RDC* radio button (determined by the customer's network administrator).
- g. Click *OK* to save the entered information, close the dialog box, and define the switch to the SAN management application.

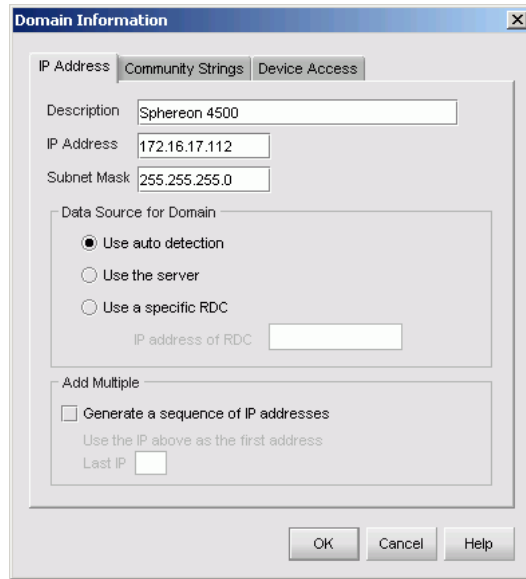


Figure D-13 Domain Information Dialog Box (IP Address Page)

- h. Click *OK* to close the *Discover Setup* dialog box and return to the SAN management application.
6. At all client backup PCs, delete all consolidated switches from the physical map (SANavigator or EFCM main window) as follows:
 - a. Right-click the Sphereon 4500 product icon (Figure D-14) representing a switch to be deleted at the SAN management application's physical map. A pop-up menu appears.



Figure D-14 Sphereon 4500 Product Icon

- b. Select the *Delete* option from the pop-up menu. The *SANavigator* or *EFCM Message* dialog box displays (Figure D-15 on page D-12).

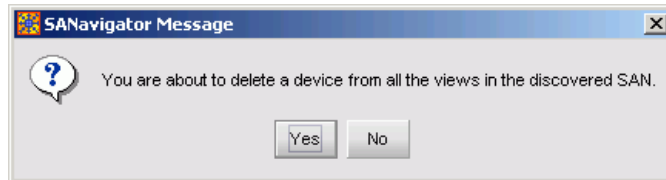


Figure D-15 SANavigator or EFCM Message Dialog Box

- c. Click *Yes* to delete the switch.
7. Daisy-chain (connect) the Ethernet hubs.
 - a. To connect the top and middle hubs in the stack, connect an RJ-45 patch cable to port **24** of the top hub, then connect the cable to port **12** of the middle hub.
 - b. To connect the bottom and middle hubs in the stack, connect a second RJ-45 patch cable to port **24** of the middle hub, then connect the cable to port **12** of the bottom hub.
 - c. Using a pencil or other pointed instrument, set the medium-dependent interface (MDI) switch on the top and middle hubs to **MDI (in)**. Set the MDI switch on the bottom hub to **MDIX (out)**. The configuration is shown in [Figure D-16](#).

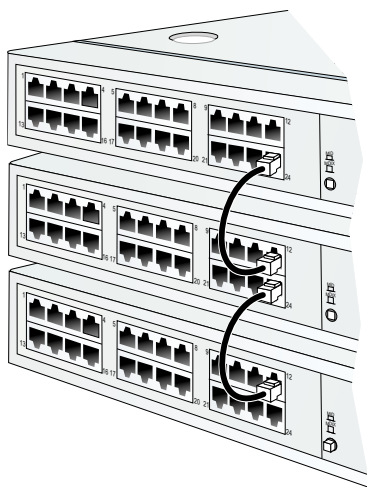


Figure D-16 Patch Cable and MDI Selector Configuration

NOTE: To connect two hubs, use [step b](#) and [step c](#) (middle and bottom hub instructions only).

8. Wait approximately five minutes for the Ethernet link to establish, then inspect the product list or physical map at the SANavigator or EFCM main window. Ensure all switch icons appear *without* a yellow triangle, red diamond, or grey square with a yellow exclamation mark, indicating the switches are defined and communicating with the SAN management application. If a problem is indicated, contact McDATA customer support.
9. If the management server is connected to a private LAN (no connection to the customer's corporate intranet), go to [Private LAN Connection](#) on page D-13. If the management server is connected to a private LAN and the customer's corporate intranet (two connections), go to [Private and Public LAN Connection](#) on page D-15.

Private LAN Connection

After completing the common steps to consolidate management server operation, recommend to the customer that the *left* RJ-45 adapter (LAN 1) at the rear of the management server and all client backup servers be disabled. This provides security and ensures against IP address conflicts because public LAN devices cannot be connected.

Disabling the Ethernet Media Adapter

Disable the LAN 1 Ethernet media adapter as follows. Repeat this step for the management server and all client backup servers.

1. At the Windows 2000 desktop, click *Start* at the left side of the task bar (bottom of the desktop), then select *Settings*, then *Control Panel*. The *Control Panel* window displays.
2. Double-click the *Network and Dial-up Connections* icon. The *Network and Dial-up Connections* window displays ([Figure D-17](#) on page D-14).

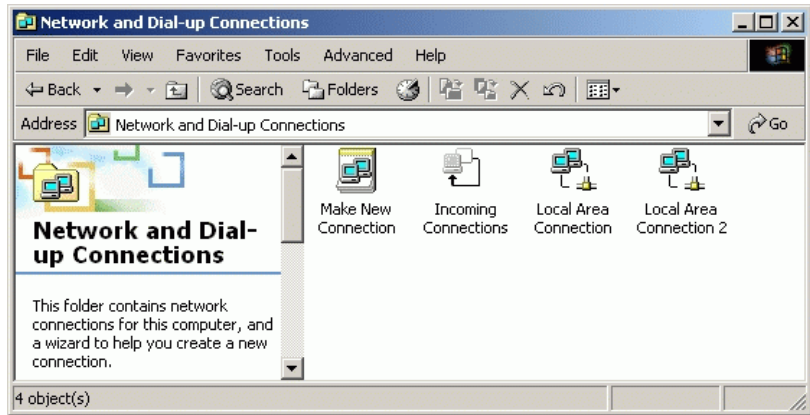


Figure D-17 Network and Dial-up Connections Window

3. Double-click the *Local Area Connection* icon. The *Local Area Connection Status* dialog box displays (Figure D-18).

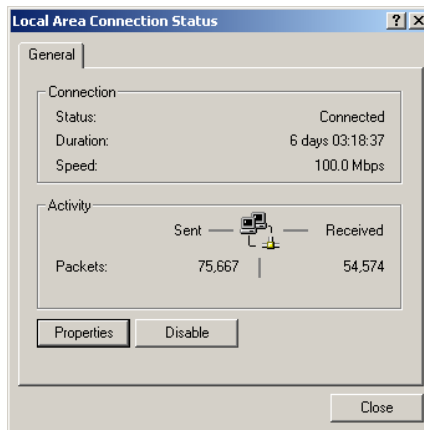


Figure D-18 Local Area Connection Status Dialog Box

4. Click *Disable*. The LAN 1 connection is disabled and the dialog box closes.

After performing the preceding steps, Figure D-19 on page D-15 shows consolidation of management servers and switches in a private LAN environment.

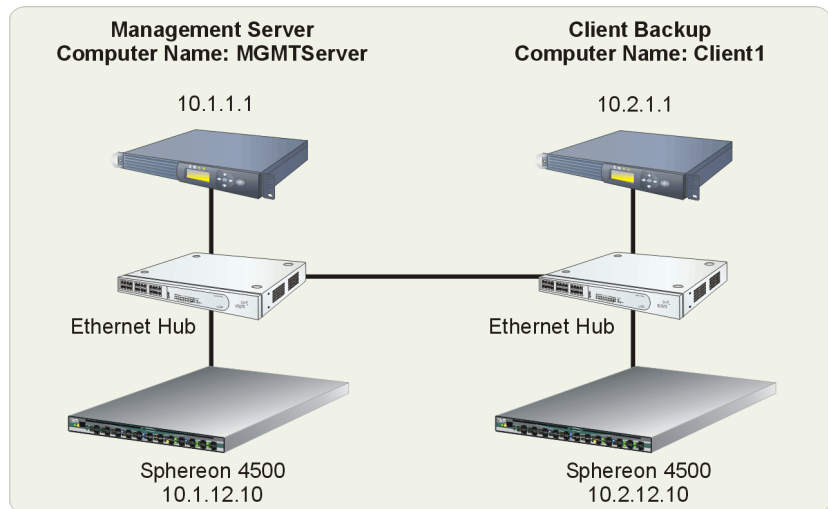


Figure D-19 Servers After Consolidation (Private LAN Connection Only)

Private and Public LAN Connection

After completing the common steps to consolidate management server operation, ensure each client backup server can login to the management server. Perform this procedure at each client backup server.

1. Reboot the client backup server at the Windows 2000 desktop (accessed through a LAN connection to a browser-capable PC):
 - a. At the Windows 2000 desktop, click *Start* at the left side of the task bar (bottom of the desktop), then select *Shut Down*. The *Shut Down Windows* dialog box displays (Figure D-20).



Figure D-20 Shut Down Windows Dialog Box

- b. Select the *Restart* option from the list box and click *OK*. The backup server powers down and restarts. During the reboot process the LAN connection between the backup server and browser-capable PC drops momentarily, and the TightVNC viewer displays a network error ([Figure D-21](#)).

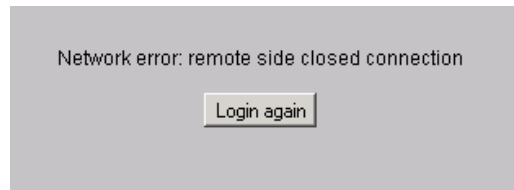


Figure D-21 TightVNC Network Error Message

- c. After the backup server reboots, click *Login again*. The *VNC Authentication* screen displays ([Figure D-22](#)).

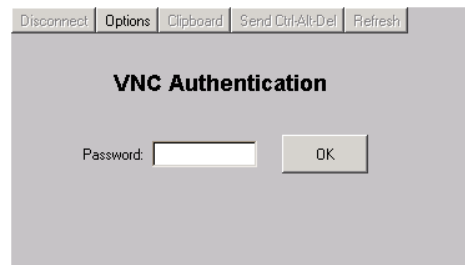


Figure D-22 VNC Authentication Screen

2. Type the default password and click *OK*. The *Welcome to Windows* dialog box displays ([Figure D-23](#) on page D-17).

NOTE: The default TightVNC viewer password is **password**.



Figure D-23 Welcome to Windows Dialog Box

3. Click the **Send Ctrl-Alt-Del** button at the top of the window to log on to the backup server desktop. The *Log On to Windows* dialog box displays (Figure D-24).

NOTE: Do not simultaneously press the **Ctrl**, **Alt**, and **Delete** keys. This action logs the user on to the browser-capable PC, not the backup server.



Figure D-24 Log On to Windows Dialog Box

4. Type the default Windows 2000 user name and password and click **OK**. The backup server's Windows 2000 desktop opens and the *SANavigator Log In* or *EFCM Log In* dialog box displays (Figure D-25 on page D-18).

NOTE: The default Windows 2000 user name is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

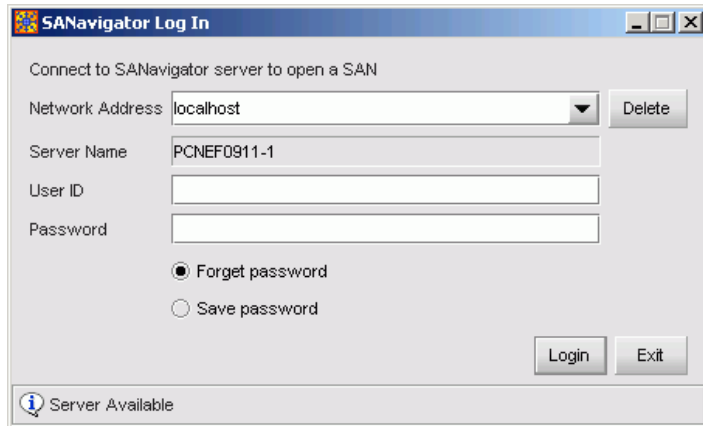


Figure D-25 SANavigator Log In or EFCM Log In Dialog Box

5. Type the SAN management application default user ID and password and select a server or IP address from the *Network Address* drop-down list.

NOTE: The default SAN management application user name is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

6. Click *Login*. The application opens and the SANavigator or EFCM main window appears.

After performing the preceding steps, [Figure D-26](#) on page D-19 shows consolidation of management servers and switches in a private and public LAN environment.

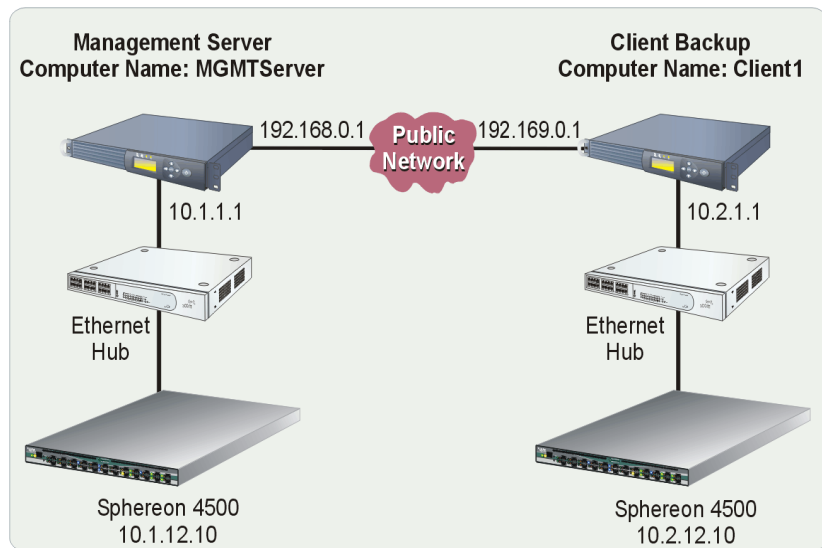


Figure D-26 Servers After Consolidation (Private and Public LAN Connections)

Reconfiguring a Client PC After a Management Server Failure

If the rack-mount management server fails, backup configuration data from the server hard drive (saved to a removable CD-ROM) is installed to any client backup server, and the client is reconfigured as the new management server.

To reconfigure a client backup server as the management server:

1. At the management server, press the power (⏻) button to power off the unit.
2. Press the left edge (**PUSH** label) of the LCD panel to disengage the panel and expose the CD-RW drive. Remove the CD with backup configuration data.
3. Insert the backup CD-ROM into the CD-RW drive of the selected client server.
4. At the Windows 2000 desktop of the client server, double-click the *My Computer* icon. The *My Computer* window displays [\(Figure D-27 on page D-20\)](#).

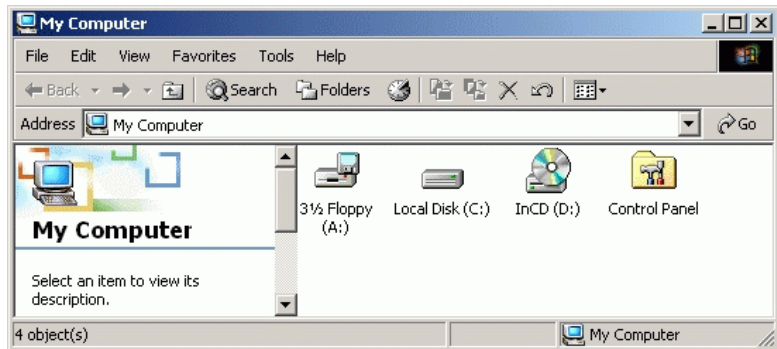


Figure D-27 My Computer Window

5. Double-click the *Local Disk (C:)* icon. The *Local Disk (C:)* window displays (Figure D-28).

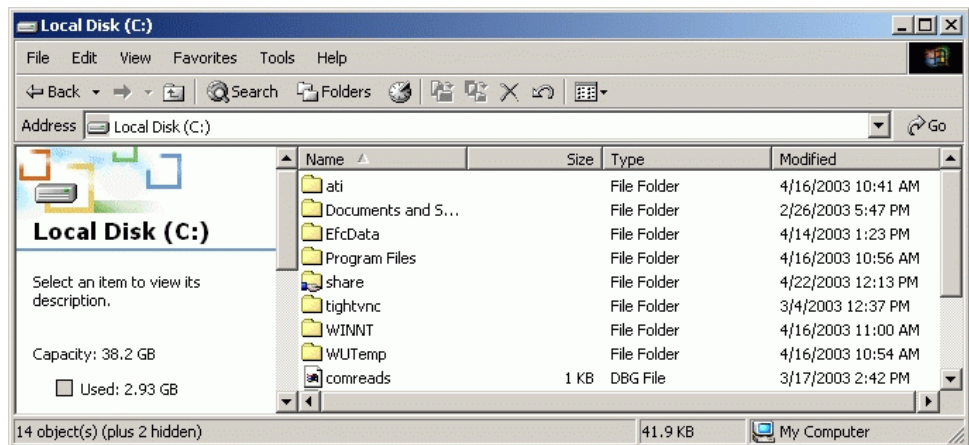


Figure D-28 Local Disk (C:) Window

6. Rename the SAN management data directories to backup directory names, then copy the following from the CD-RW drive to the hard drive (local disk) as a replacement:

- For the Sanavigator 4.0 application, copy the backup CD-ROM contents to the following directories:
 - C:\Program Files\SANavigator4.0\CallHome
 - C:\Program Files\SANavigator4.0\Client
 - C:\Program Files\SANavigator4.0\Server.
 - For the EFCM 8.0 application, copy the backup CD-ROM contents to the following directories:
 - C:\Program Files\EFCM 8.0\CallHome
 - C:\Program Files\EFCM 8.0\Client
 - C:\Program Files\EFCM 8.0\Server.
7. Click close (X) at the upper right corner of the *Local Disk (C:)* and *My Computer* windows to close the windows and return to the Windows 2000 desktop.
 8. Leave the CD in the CD-RW drive for backup purposes.

ATTENTION ! Contents of the data directory are backed up to the management server's CD-RW drive when directory contents change. To ensure trouble-free backups, always leave a CD in the drive. Ensure data is not being written to or read from the CD-RW drive before removing the CD. Removing the CD during a backup or restore operation can corrupt data.

9. Reboot the client backup server (new management server) as follows:
 - a. At the Windows 2000 desktop, click *Start* at the left side of the task bar, then select *Shut Down*. The *Shut Down Windows* dialog box displays (Figure D-20 on page D-15).
 - b. Select the *Restart* option from the list box and click *OK*. The backup server powers down and restarts. During the reboot process the LAN connection between the backup server and browser-capable PC drops momentarily, and the TightVNC viewer displays a network error (Figure D-21 on page D-16).
 - c. After the backup server reboots, click *Login again*. The *VNC Authentication* screen displays (Figure D-22 on page D-16).

10. Type the default password and click *OK*. The *Welcome to Windows* dialog box displays (Figure D-23 on page D-17).

NOTE: The default TightVNC viewer password is **password**.

11. Click the **Send Ctrl-Alt-Del** button at the top of the window to log on to the backup server desktop. The *Log On to Windows* dialog box displays (Figure D-24 on page D-17).

NOTE: Do not simultaneously press the **Ctrl**, **Alt**, and **Delete** keys. This action logs the user on to the browser-capable PC, not the backup server.

12. Type the default Windows 2000 user name and password and click *OK*. The backup server's Windows 2000 desktop opens and the *SANavigator Log In* or *EFCM Log In* dialog box displays (Figure D-25 on page D-18).

NOTE: The default Windows 2000 user name is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

13. Type the SAN management application default user ID and password and select a server or IP address from the *Network Address* drop-down list.

NOTE: The default SAN management application user name is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

14. Click *Login*. The application opens and the SANavigator or EFCM main window appears.

A

- applications
 - Element Manager [1-21](#)
 - SAN management [1-19](#)
 - SANpilot interface [1-17](#)
- attention statements [xxiv](#)
- audit log
 - Element Manager application [4-16](#)
 - SAN management application [4-13](#)

B

- back up
 - SAN management application configuration data [2-115](#)
 - switch configuration file [4-79](#)
- binding
 - fabric
 - configure [2-34](#)
 - description [2-34](#)
 - port
 - configure [2-31, 2-103](#)
 - description [2-31](#)
 - switch
 - configure [2-32, 2-96](#)
 - description [2-32, 2-96](#)
 - disable [2-32, 2-97](#)
 - enable [2-32, 2-97](#)
 - online state requirements [2-96](#)
 - zoning requirements [2-97](#)
- block ports
 - from management server [4-52](#)
 - from SANpilot interface [4-51](#)

C

- call-home support
 - configure at management server [2-71, 2-114](#)
 - description [1-23](#)
 - enable at management server [2-114](#)
- clean fiber-optic components [4-54](#)
- clear
 - event log entries [4-8, 4-9, 4-10, 4-12, 4-13](#)
 - port statistics [4-25](#)
- clearances [1-8](#)
- client PC
 - description [1-12](#)
 - specifications [1-14](#)
- client workstation
 - description [1-12](#)
 - specifications [1-14](#)
- CNT WAN support
 - description [2-39](#)
 - PFE key [2-39, 2-82](#)
- command line interface
 - disable at SANpilot interface [2-28](#)
 - enable at SANpilot interface [2-28](#)
- compliance statements
 - Class 1 laser transceiver [xxii](#)
 - CNS mark [xxiii](#)
 - European Union conformity declarations [xxiii](#)
 - European Union directives [xxiii](#)
 - Federal Communications Commission [xxii](#)
- configuration file
 - back up [4-79](#)
 - restore [4-80](#)
- configure

- call-home feature 2-71
- call-home support 2-114
- e-mail notification 2-112
- Ethernet events 2-114
- fabric binding 2-34
- fabric parameters 2-21, 2-92
- management server date and time 2-69
- management server DNS domain name 2-55
- management server IP address 2-51
- management server name 2-55
- management server password 2-51
- management server subnet mask 2-51
- OpenTrunking 2-36, 2-109
- OSMS 2-29
- passwords 2-30, 2-51, 2-72
- PFE key 2-38, 2-82
- port binding 2-31, 2-103
- ports 2-15, 2-101
- preferred path 2-94
- SNMP 2-26, 2-103
- switch binding 2-32, 2-96
- switch date and time 2-18, 2-86
- switch identification 2-17, 2-89
- switch network information 2-24, 2-41
- switch operating parameters 2-19, 2-90
- switch to SAN management application 2-76
- threshold alerts 2-105
- user names 2-30, 2-72
- Windows 2000 users 2-63
- zone sets 2-121
- zones 2-121
- consolidating management servers
 - IP address assignment D-3
 - overview D-1
 - private LAN connection D-13
 - procedure D-5
 - public LAN connection D-15
 - requirements D-3
- cooling fan
 - description 1-5
 - events (300 - 399) B-23
 - fault isolation 3-68
 - illustrated parts breakdown 6-3
- counter 4-25
- CTP card
 - events (400 - 499) B-29
 - fault isolation 3-68

- firmware versions 4-59

D

- danger statements xxiv
- data collection procedure
 - management server 4-47
 - SANpilot interface 4-45
- date
 - set at management server 2-69
 - set switch date at management server 2-86
 - set switch date at SANpilot interface 2-18
- default
 - DNS server IP address 2-78
 - maintenance port password 2-44
 - management server gateway address 2-78
 - management server IP address 2-78
 - management server LCD panel password 2-51
 - management server subnet mask 2-78
 - SAN management application password 2-72, 2-120, 4-94, C-7, D-18, D-22
 - SAN management application user name 2-72, 2-120, 4-94, C-7, D-18, D-22
 - SANpilot interface password 2-15
 - SANpilot interface user name 2-15
 - switch gateway address 2-1, 3-1
 - switch IP address 2-1, 3-1
 - switch passwords 2-1, 3-1
 - switch subnet mask 2-1, 3-1
 - TightVNC password 2-56, 2-119, 4-93, C-5, D-16, D-22
 - Windows 2000 password 2-58, 2-119, 4-94, C-6, D-18, D-22
 - Windows 2000 user name 2-58, 2-119, 4-94, C-6, D-18, D-22
- definition
 - wraps 4-25
- dimensions 1-7
- download firmware
 - from file center 4-60, 4-69
 - through management server 4-76
 - through SANpilot interface 4-66

E

- E_D_TOV 2-22, 2-93
- E_Port

- configuring 2-15, 2-101
 - description 1-2
 - segmented 3-93
 - Element Manager application
 - audit log 4-16
 - configuring 2-88
 - description 1-21
 - error messages A-1
 - event log 4-16
 - hardware log 4-17
 - Hardware View 1-22
 - information messages A-1
 - link incident log 4-18
 - PFE key 2-82
 - threshold alert log 4-19
 - e-mail support
 - configure at management server 2-112
 - description 1-23
 - enable at management server 2-112
 - enable
 - call-home support 2-114
 - CLI 2-28
 - EFM 2-35, 2-97
 - e-mail notification 2-112
 - Ethernet events 2-114
 - fabric binding 2-34
 - host control 2-29
 - port binding 2-31, 2-103
 - SANpilot interface 2-112
 - switch binding 2-32, 2-97
 - Telnet access 2-112
 - enterprise fabric mode
 - enable at SAN management application 2-97
 - enable at SANpilot interface 2-35
 - environment
 - operating 1-9
 - shipping 1-8
 - storage 1-8
 - ERR LED
 - description 1-6
 - location 1-3
 - error
 - log, clearing 4-8, 4-9, 4-10, 4-12, 4-13
 - statistics 4-27
 - error detection
 - description 1-15
 - event codes 3-2
 - SANpilot interface 1-17
 - error messages
 - Element Manager application A-1
 - error reporting
 - description 1-15
 - event codes 3-2
 - SANpilot interface 1-17
 - ESD precautions xxviii
 - Ethernet connector
 - description 1-6
 - location 1-3
 - Ethernet events
 - configure at management server 2-114
 - enable at management server 2-114
 - Ethernet hub
 - description 1-12
 - fault isolation 3-51
 - illustration 1-12
 - installation 2-5
 - event codes
 - cooling fan events (300 - 399) B-23
 - CTP card events (400 - 499) B-29
 - description B-2
 - port events (500 - 599) B-35
 - power supply events (200 - 299) B-20
 - system events (000 - 199) B-2
 - thermal sensor events (800 - 899) B-43
 - event log 4-7, 4-8, 4-9, 4-10, 4-12
 - clearing 4-8, 4-9, 4-10, 4-12, 4-13
 - Element Manager application 4-16
 - SAN management application 4-13
 - SANpilot interface 4-4
 - external loopback test
 - description 4-38
 - from management server 4-43
 - from SANpilot interface 4-40
- ## F
- F_Port
 - configuring 2-15, 2-101
 - description 1-2
 - fabric binding
 - configure 2-34
 - description 2-34
 - fabric log 4-16
 - fabric parameters

- configure at management server [2-92](#)
 - configure at SANpilot interface [2-21](#)
 - Fabriccenter equipment cabinet
 - description [1-2](#)
 - Ethernet hub installation [2-8](#)
 - management server installation [2-48](#)
 - switch installation [2-12](#)
 - fault isolation
 - MAP 0000 - Start MAP [3-6](#)
 - MAP 0100 - Power distribution analysis [3-30](#)
 - MAP 0200 - POST failure analysis [3-38](#)
 - MAP 0300 - Server application problem determination [3-41](#)
 - MAP 0400 - Loss of server communication [3-51](#)
 - MAP 0500 - FRU failure analysis [3-68](#)
 - MAP 0600 - Port failure and link incident analysis [3-74](#)
 - MAP 0700 - Fabric, ISL, and segmented port problem determination [3-93](#)
 - MAP 0800 - Server hardware problem determination [3-110](#)
 - summary [3-2](#)
 - FCC compliance statement [xxii](#)
 - fiber-optic protective plug
 - description [1-25](#)
 - illustration [1-25](#)
 - file center
 - download firmware to browser PC [4-60](#)
 - download firmware to management server library [4-69](#)
 - download SAN management application [4-87](#)
 - registration [2-127](#)
 - firmware
 - add version to browser PC [4-60](#)
 - add version to management server library [4-69](#)
 - determine version at management server [4-68](#)
 - determine version at SANpilot interface [4-60](#)
 - download through management server [4-76](#)
 - download through SANpilot interface [4-66](#)
 - download version from file center [4-60, 4-69](#)
 - FL_Port
 - configuring [2-15, 2-101](#)
 - description [1-2](#)
 - Flexport Technology PFE key [2-39, 2-82](#)
 - frames
 - too short, error statistics [4-27](#)
 - FRU removal
 - power supply [5-6](#)
 - SFP transceiver [5-2](#)
 - tools required [5-2, 5-6](#)
 - FRU replacement
 - power supply [5-8](#)
 - SFP transceiver [5-4](#)
 - tools required [5-2, 5-6](#)
 - FRUs
 - description [1-3](#)
 - illustrated parts breakdown [6-1](#)
 - power supply [1-5](#)
 - SFP transceiver [1-4](#)
 - status LEDs [1-7](#)
 - full-volatility feature
 - description [4-44](#)
 - PFE key [2-39, 2-82](#)
- ## G
- gateway address
 - change switch address [2-24, 2-41](#)
 - management server default [2-78](#)
 - switch default [2-1, 3-1](#)
- ## H
- hardware log [4-17](#)
 - Hardware View [1-22](#)
- ## I
- identification
 - configure at management server [2-89](#)
 - configure at SANpilot interface [2-17](#)
 - illustrated parts breakdown
 - front-accessible FRUs [6-2](#)
 - miscellaneous parts [6-4](#)
 - power cords [6-5](#)
 - rear-accessible FRUs [6-3](#)
 - IML switch [4-57](#)
 - IML/Reset button
 - function [1-6](#)
 - location [1-3](#)
 - information messages

- Element Manager application [A-1](#)
- insistent domain ID [2-21, 2-91](#)
- installation options
 - customer-supplied rack [2-3](#)
 - desktop [2-2](#)
 - Fabriccenter cabinet [2-2](#)
- installation tasks
 - summary [2-3](#)
 - Task 1 - Verify installation requirements [2-4](#)
 - Task 10 - Set management server date and time [2-69](#)
 - Task 11 - Configure the call-home feature (optional) [2-71](#)
 - Task 12 - Assign user names and passwords [2-72](#)
 - Task 13 - Configure the switch to the management application [2-76](#)
 - Task 14 - Record or verify server restore information [2-78](#)
 - Task 15 - Verify switch-to-server communication [2-80](#)
 - Task 16 - Configure PFE key (optional) [2-82](#)
 - Task 17 - Configure management server (optional) [2-86](#)
 - Task 18 - Set switch date and time [2-86](#)
 - Task 19 - Configure the Sphereon 4500 Element Manager application [2-88](#)
 - Task 2 - Unpack, inspect, and install the Ethernet hub (optional) [2-5](#)
 - Task 20 - Back up configuration data [2-115](#)
 - Task 21 - Cable Fibre Channel ports [2-120](#)
 - Task 22 - Configure zoning (optional) [2-121](#)
 - Task 23 - Connect switch to a fabric element (optional) [2-125](#)
 - Task 24 - Register with the McDATA file center [2-127](#)
 - Task 3 - Unpack, inspect, and install the switch [2-10](#)
 - Task 4 - Configure the switch at the SANpilot interface (optional) [2-13](#)
 - Task 5 - Configure switch network information (optional) [2-41](#)
 - Task 6 - Unpack, inspect, and install the management server [2-47](#)
 - Task 7 - Configure server password and network addresses [2-51](#)

- Task 8 - Configure management server information [2-55](#)
- Task 9 - Configure Windows 2000 users [2-63](#)
- internal loopback test
 - description [4-38](#)
 - from management server [4-41](#)
 - from SANpilot interface [4-38](#)
- interop mode [2-23, 2-93](#)
- interswitch link
 - description [1-2](#)
 - fault isolation [3-93](#)
- IP address
 - change switch address [2-24, 2-41](#)
 - consolidating management servers [D-3](#)
 - DNS server default [2-78](#)
 - management server default [2-78](#)
 - switch default [2-1, 3-1](#)
- IPL switch [4-58](#)

L

- LAN connection
 - connect the management server [2-47](#)
 - consolidating management servers [D-13, D-15](#)
- laser transceiver
 - compliance statement [xxii](#)
 - description [1-4](#)
 - illustrated parts breakdown [6-2](#)
 - removal [5-2](#)
 - replacement [5-4](#)
 - types available [1-4](#)
- LCD panel
 - configure private management server network addresses [2-52](#)
 - configure public management server network addresses [2-54](#)
 - default password for management server [2-51](#)
- LEDs
 - ERR [1-6](#)
 - port status [1-7, 4-21](#)
 - power supply status [1-7](#)
- link incident log
 - Element Manager application [4-18](#)
 - SANpilot interface [4-6](#)
- log

- clearing [4-8, 4-9, 4-10, 4-12, 4-13](#)
- events [4-7, 4-8, 4-9, 4-10, 4-12](#)
- Log tab view [4-7, 4-8, 4-9, 4-10, 4-12](#)
- logs
 - Element Manager link incident [4-18](#)
 - fabric [4-16](#)
 - hardware [4-17](#)
 - product status [4-14](#)
 - SAN management application audit [4-13](#)
 - SAN management application event [4-13](#)
 - SANpilot event [4-4](#)
 - SANpilot link incident [4-6](#)
 - SANpilot open trunking [4-5](#)
 - session [4-14](#)
 - Sphereon 4500 audit [4-16](#)
 - Sphereon 4500 event [4-16](#)
 - threshold alert [4-19](#)
- loopback plug
 - description [1-24](#)
 - illustration [1-24](#)
- loopback test
 - description [4-38](#)
 - external, management server [4-43](#)
 - external, SANpilot interface [4-40](#)
 - internal, management server [4-41](#)
 - internal, SANpilot interface [4-38](#)

M

- MAC address, switch [2-41](#)
- maintenance analysis procedures
 - MAP 0000 - Start MAP [3-6](#)
 - MAP 0100 - Power distribution analysis [3-30](#)
 - MAP 0200 - POST failure analysis [3-38](#)
 - MAP 0300 - Server application problem determination [3-41](#)
 - MAP 0400 - Loss of server communication [3-51](#)
 - MAP 0500 - FRU failure analysis [3-68](#)
 - MAP 0600 - Port failure and link incident analysis [3-74](#)
 - MAP 0700 - Fabric, ISL, and segmented port problem determination [3-93](#)
 - MAP 0800 - Server hardware problem determination [3-110](#)
 - summary [3-2](#)
- maintenance approach [1-9](#)

- maintenance port
 - configure switch network addresses [2-42](#)
 - default password [2-44](#)
 - description [1-7](#)
 - location [1-4](#)
- management
 - client PC or workstation [1-12](#)
 - management server [1-11](#)
 - SANpilot interface [1-11](#)
- management server
 - access desktop through TightVNC [2-55](#)
 - consolidating servers [D-5](#)
 - description [1-11](#)
 - event code tables [B-1](#)
 - fault isolation [3-51](#)
 - hardware fault isolation [3-110](#)
 - illustration [1-11](#)
 - installation [2-47](#)
 - LCD panel password [2-51](#)
 - reconfigure client [D-19](#)
 - restore procedure [C-2](#)
 - restore requirements [C-1](#)
 - specifications [1-11](#)
- monitoring
 - events [4-7, 4-8, 4-9, 4-10, 4-12](#)

N

- network information
 - configure management server [2-51](#)
 - configure switch at management server [2-41](#)
 - configure switch at SANpilot interface [2-24](#)

- null modem cable
 - description [1-25](#)
 - illustration [1-25](#)

O

- offline state
 - set from management server [4-50](#)
 - set from SANpilot interface [4-49](#)
- online state
 - set from management server [4-50](#)
 - set from SANpilot interface [4-49](#)
- open trunking log
 - SANpilot interface [4-5](#)
- open-systems management server
 - configure [2-86](#)

- configure at SANpilot interface [2-29](#)
 - PFE key [2-39, 2-82](#)
- OpenTrunking
 - configure at management server [2-109](#)
 - configure at SANpilot interface [2-36](#)
- OpenTrunking PFE key [2-39, 2-82](#)
- operating environment [1-9](#)
- operating parameters
 - configure at management server [2-90](#)
 - configure at SANpilot interface [2-19](#)
- P**
- password
 - configure at management server [2-72](#)
 - configure at SANpilot interface [2-30](#)
 - customer-level switch [2-1, 3-1](#)
 - default
 - management server LCD panel [2-51](#)
 - default maintenance port [2-44](#)
 - default SAN management application [2-72, 2-120, 4-94, C-7, D-18, D-22](#)
 - default SANpilot interface [2-15](#)
 - default TightVNC [2-56, 2-119, 4-93, C-5, D-16, D-22](#)
 - default Windows 2000 [2-58, 2-119, 4-94, C-6, D-18, D-22](#)
 - maintenance-level switch [2-1, 3-1](#)
- performance statistics
 - Class 2 [4-33](#)
 - Class 3 [4-34](#)
 - error [4-34](#)
 - operational [4-35](#)
 - traffic [4-35](#)
- PFE keys
 - CNT WAN support [2-39, 2-82](#)
 - configure at management server [2-82](#)
 - configure at SANpilot interface [2-38](#)
 - Element Manager application [2-82](#)
 - Flexport Technology feature [2-39, 2-82](#)
 - full-volatility feature [2-39, 2-82](#)
 - open-systems management server [2-39, 2-82](#)
 - OpenTrunking [2-39, 2-82](#)
 - SANtegrity binding [2-39, 2-82](#)
- port
 - clear statistics [4-25](#)
- port binding
 - configure [2-31, 2-103](#)
 - description [2-31](#)
- ports
 - block [4-51](#)
 - cabling [2-120](#)
 - configurable types [1-2](#)
 - configure at management server [2-101](#)
 - configure at SANpilot interface [2-15](#)
 - diagnostics [4-21](#)
 - events (500 - 599) [B-35](#)
 - loopback test [4-38](#)
 - performance statistics [4-24, 4-32](#)
 - port properties [4-28, 4-35](#)
 - port technology [4-28, 4-37](#)
 - SFP transceivers [1-4](#)
 - status LEDs [1-7, 4-21](#)
 - unblock [4-51](#)
- power cords
 - connecting [2-11](#)
 - illustrated parts breakdown [6-5](#)
- power requirements [1-7](#)
- power supply
 - description [1-5](#)
 - events (200 - 299) [B-20](#)
 - fault isolation [3-30](#)
 - illustrated parts breakdown [6-3](#)
 - removal [5-6](#)
 - replacement [5-8](#)
 - status LED [1-7](#)
- power-off procedure [4-56](#)
- power-on procedure [4-55](#)
- precautions
 - ESD [xxviii](#)
 - general [xxviii](#)
- preferred domain ID [2-20, 2-91](#)
- preferred path [2-94](#)
- procedural notes [4-2, 5-1](#)
- procedures
 - data collection [4-44](#)
 - fault isolation [3-1](#)
 - FRU remove and replace [5-2](#)
 - installation [2-3](#)
 - power-off [4-56](#)
 - power-on [4-55](#)
 - repair [4-1](#)
- product status log [4-14](#)
- publications, related [xx](#)

PWR LED

- description 1-6
- location 1-3

R

R_A_TOV 2-22, 2-92

rack-mount installation

- Ethernet hub 2-8
- management server 2-48
- Sphereon 4500 Switch 2-12

reconfigure client PC D-19

remove and replace procedures 5-2

repair procedures

- block or unblock a port 4-51
- clean fiber-optic components 4-54
- collect maintenance data 4-44
- IML, IPL, or reset the switch 4-56
- install or upgrade software 4-87
- manage configuration data 4-79
- manage firmware versions 4-59
- obtain log information 4-2
- obtain port diagnostic information 4-21
- overview 4-1
- perform port diagnostic loopback tests 4-38
- power-off procedure 4-56
- power-on procedure 4-55
- set the switch online or offline 4-48

rerouting delay 2-21, 2-91

reset

- configuration data from management server 4-84
- configuration data from SANpilot interface 4-82
- switch 4-58

restore

- management server C-2
- switch configuration file 4-80

S

safety

- attention statements xxiv
- danger statements xxiv
- ESD precautions xxviii
- general precautions xxviii

SAN management application

- audit log 4-13

- default password 2-72, 2-120, 4-94, C-7, D-18, D-22

- default user name 2-72, 2-120, 4-94, C-7, D-18, D-22

- description 1-19
- event log 4-13
- fabric log 4-16
- main window 1-19, 2-73
- product status log 4-14
- session log 4-14

SANpilot interface

- configure a switch 2-13
- default display 1-17
- description 1-11
- disable at management server 2-112
- enable at management server 2-112
- event log 4-4
- link incident log 4-6
- open trunking log 4-5
- server hardware fault isolation 3-110

SANtegrity binding PFE key 2-39, 2-82

segmented E_Port

- description 2-20, 2-91
- fault isolation 3-93

serviceability features 1-15

session log 4-14

SFP transceiver

- description 1-4
- fault isolation 3-74
- illustrated parts breakdown 6-2
- removal 5-2
- replacement 5-4
- types available 1-4

shipping environment 1-8

SNMP

- configure at management server 2-103
- configure at SANpilot interface 2-26
- description 1-23
- traps 1-23

software

- diagnostic features 1-17
- download SAN management application from file center 4-87
- Element Manager application 1-21
- install 4-87
- SAN management application 1-19
- SANpilot interface 1-17

- upgrade 4-87
- Solution Center
 - e-mail address [xxi](#)
 - fax number [xxi](#)
 - phone number [xxi](#)
- specifications
 - client PC 1-14
 - client workstation 1-14
 - management server 1-11
 - management server consolidation [D-3](#)
 - switch clearances 1-8
 - switch dimensions 1-7
 - switch power requirements 1-7
- Sphereon 4500 Switch
 - description 1-2
 - firmware 4-59
 - FRU removal and replacement 5-1
 - FRUs 1-3
 - illustrated parts breakdown 6-1
 - illustration 1-2
 - installation 2-10
 - installation options 2-2
 - maintenance analysis procedures 3-1
 - maintenance approach 1-9
 - management 1-10
 - repair procedures 4-1
 - specifications 1-7
- statistics
 - clear for port 4-25
 - counter 4-25
 - wraps 4-25
- storage environment 1-8
- subnet mask
 - change switch value 2-24, 2-41
 - management server default 2-78
 - switch default 2-1, 3-1
- switch binding
 - configure 2-32, 2-97
 - description 2-32, 2-96
 - disable 2-97
 - enable 2-97
 - online state requirements 2-96
 - zoning requirements 2-97
- switch priority 2-23, 2-93
- system events (000 - 199) [B-2](#)

T

- technical support
 - file center registration 2-127
 - Solution Center e-mail address [xxi](#)
 - Solution Center fax number [xxi](#)
 - Solution Center phone number [xxi](#)
- Telnet access
 - disable at management server 2-112
 - enable at management server 2-112
- test
 - call-home support 2-114
 - e-mail notification 2-112
- thermal sensor events (800 - 899) [B-43](#)
- threshold alert log 4-19
- threshold alerts
 - configure 2-105
 - types 2-106
- TightVNC
 - access management server desktop 2-55
 - default password 2-56, 2-119, 4-93, C-5, D-16, [D-22](#)
- time
 - set at management server 2-69
 - set switch time at management server 2-86
 - set switch time at SANpilot interface 2-18
- tools and test equipment
 - FRU removal and replacement 5-2, 5-6
 - supplied by service personnel 1-25
 - supplied with switch 1-24
- trademarks [xxii](#)

U

- unblock ports
 - from management server 4-53
 - from SANpilot interface 4-52
- user name
 - configure at management server 2-72
 - configure at SANpilot interface 2-30
 - default SAN management application 2-72, 2-120, 4-94, C-7, D-18, D-22
 - default SANpilot interface 2-15
 - default Windows 2000 2-58, 2-119, 4-94, C-6, D-18, D-22

V

verify

- management server restore information [2-78](#)
- power supply replacement [5-10](#)
- SFP transceiver replacement [5-5](#)
- switch-to-server communication [2-80](#)

W

Windows 2000

- configure users [2-63](#)
 - default password [2-58, 2-119, 4-94, C-6, D-18, D-22](#)
 - default user name [2-58, 2-119, 4-94, C-6, D-18, D-22](#)
- wraps, definition [4-25](#)

Z

zone sets

- configure at SANpilot interface [2-124](#)
- description [2-121](#)

zones

- add or delete members [2-123](#)
- configure at SANpilot interface [2-121](#)
- description [2-121](#)